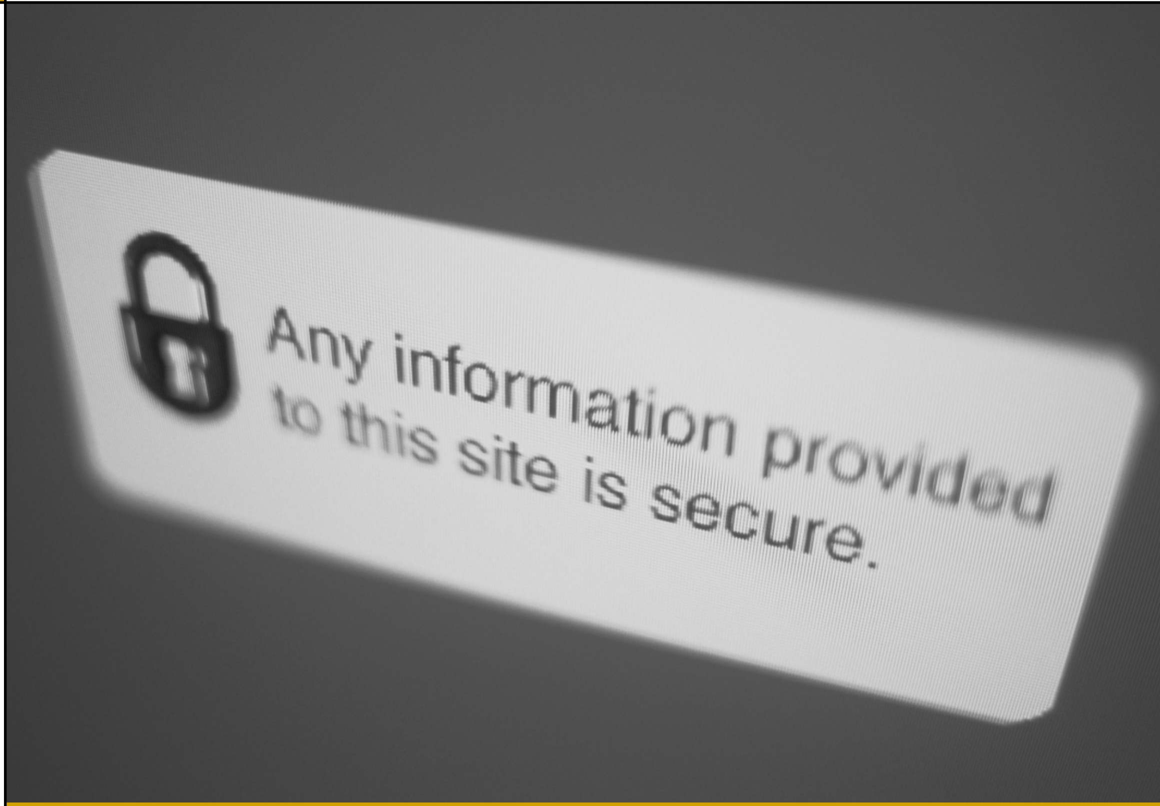
SECOND EDITION
OCTOBER 2002

Public-Sector Information Security: A Call to Action for Public-Sector CIOs



Any information provided to this site is secure.

E-Government Series

Don Heiman
National Association of State Chief Information Officers (NASCIO)

IBM Endowment for
The Business of Government

Report Documentation Page

Report Date 01OCT2002	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Public-Sector Information Security: A Call to Action for Public-Sector CIOs	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) National Association of State Chief Information Officers (NASCIO)	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 48	

E-GOVERNMENT SERIES

Public-Sector Information Security: A Call to Action for Public-Sector CIOs

Don Heiman
National Association of State Chief Information Officers (NASCIO)

October 2002

TABLE OF CONTENTS

FOREWORD

October 2002

On behalf of the IBM Endowment for The Business of Government, we are pleased to present this report by Don Heiman, "Public-Sector Information Security: A Call to Action for Public-Sector CIOs."

This report expands upon the themes and issues raised at a forum on Security and Critical Infrastructure Protection sponsored by the National Association of State Chief Information Officers (NASCIO) with the support of the IBM Endowment. Forum participants included state chief information officers, government information technology managers, and other key state government staff. At the forum, held in November 2001, conference participants identified a series of actions designed to combat emerging cyber-threats to security and critical infrastructure.

Subsequent to the forum, NASCIO asked Don Heiman, former chief information officer of the State of Kansas, to develop recommendations for improving public-sector information security. He developed 10 recommendations in three areas: management, technology, and homeland security. Taken together, these recommendations reflect the concept that security is about more than just information technology. One key point is that IT governance is a critical responsibility for the heads of government entities and should include all key stakeholders.

The report argues that in order to exercise effective enterprise and IT governance, agency heads and the agency's executive management team must have a clear understanding of what to expect from their enterprise's information and security programs. It is crucial that organizations evaluate the positive aspects and shortcomings of their current security program, and then design improved programs to meet organizational needs. Organizations also must work to improve their capacity to effectively implement their security program.

The 10 recommendations set forth by Heiman are critical components to a successful response against cyber-security threats and attacks. We trust that this report will be helpful and useful to chief information officers at all levels of government as they develop and implement security measures to protect the nation's critical infrastructure.

Paul Lawrence Co-Chair, IBM Endowment for The Business of Government	Ian Littman Co-Chair, IBM Endowment for The Business of Government

EXECUTIVE SUMMARY

"The U.S. must come to terms with the six lessons of cyber-security: 1. We have enemies.… 2. They are smart. Thus, we shouldn't underestimate them.… 3. They will use our technology against us, especially if they understand it better than we do.… 4. They will attack the seams of our technology infrastructure.… 5. Our technology, like our society, is surprisingly interdependent.… 6. The only way to counter this threat is for all levels of government and the private sector to work together."[1]

—Richard Clarke
Special Advisor on Cybersecurity
White House Office of Homeland Security

In November 2001, the National Association of State Chief Information Officers (NASCIO) sponsored the Forum on Security and Critical Infrastructure Protection, funded by a grant from The IBM Endowment for The Business of Government. More than 80 individuals participated in the day-and-a-half event. Participants included state chief information officers (CIOs) and security chiefs representing 35 states. Other participants included representatives of local and federal government information technology (IT) management as well as other agencies and branches of state government. A summary of the proceedings of that forum can be found in Appendix I.

This report represents a call to action built, in part, upon the results of that forum. Specifically, the report calls public-sector CIOs to act on the following 10 recommendations:

Management:

1. Make sure everyone is at the table. Develop an IT governance structure that is inclusive of all stakeholders. The structure should include security governance at the enterprise level and it should bring to the policy table emergency response and audit leadership. All branches of state government and local units of government should be represented in order to develop policies, set standards, and establish enterprise-level security plans.
2. Develop measures for enterprise success. Implement enterprise planning for security outcomes, including measures for success and best practices for setting and performing tasks, and commit to sharing resources for the good of the whole.
3. Adopt IT control objectives to manage, implement, and maintain IT systems.
4. Develop security metrics that accurately measure unwanted intrusions, security breaches, penetrations, and vulnerabilities. The reporting

should be shared at a summary level with the executive, legislative, and judicial branches of state government as well as with other governmental organizations. The reports should be confidential to government communities.

5. Develop state enterprise-IT architectures that include security as an underlying domain with disciplines based on engineering standards, best practices, and accepted architecture-setting methodologies. The architectures should underlie the various IT domains and include physical security.

6. Develop a business case for security based on a full risk assessment of critical-infrastructure vulnerabilities. The risk assessment should include a complete inventory of critical systems and assets. It should also involve a gap analysis between actual and ideal security levels for the identified systems and related assets.

Technology:

7. Deploy automated and manual security technologies based on asset inventories and application criticality, including security levels derived from the enterprise architecture for IT.

8. Develop a state security portal that integrates with emerging technologies for emergency response such as intelligent roads and radio-frequency infrastructure. The state security portal should have a public access site as well as a private enterprise site for coordinating emergency response.

Homeland Security:

9. Establish an interstate security information sharing and analysis center (interstate ISAC) funded at least partially by the federal government. The interstate ISAC, building on the federal-sector ISAC model, will assist states in analyzing security breaches, repairing affected systems, reporting security alerts, providing clearinghouse services for progressive practices, and interfacing with appropriate federal entities.

10. Develop model state legislation that allows local, state, and federal entities to confidentially share security incident reports among themselves and with other ISACs supporting the nation’s critical-infrastructure owners and operators.

These recommendations are essential to any successful response to increasing incidents of cybersecurity threats and attacks.

Introduction

Public-sector chief information officers (CIOs) at all levels operate on the boundary line between their governments' internal organizations and those external forces that threaten their systems—some of our nation's most critical infrastructure. Security is implemented on this boundary line. At the end of this report (Appendix II), you will read about Mark's story. Mark is a state senior technologist, and his story is a composite of collective experiences and scenarios. However, in a larger sense, it is a story for all public-sector CIOs, a story both prophetic and sobering. Deep in this story, however, there is also a message about the satisfaction and enjoyment that comes from meeting difficult challenges.

Security is more than a principle or a right. If implemented properly, security is a way of life. It protects basic values that underpin our culture and liberties. This report is about security of information technology (IT), our way of life, and the values that lay deep in the core of our American culture. These values include rights to personal privacy, assurance of liberty, mutual and self-protection, and basic economic and social freedoms central to our democracy. This report is oriented toward a special audience of government CIOs in local, state, and federal jurisdictions. More than anything else, this report is a call to action, written with a sense of urgency and dedicated to the victims and families of the September 11th attacks on America.

Today government is uniquely accessible and federated. The federation of hundreds of agencies and their accessibility makes it difficult for governments to adopt common IT architectures and management (audit) standards. In addition, many states do not have security-confidentiality laws. This inhibits information sharing about security breaches and unwelcome intrusions across branches of government and jurisdictions. Also, states do not have security risk assessments on all their critical IT assets. This thwarts their ability to develop metrics and report on security performance. Finally, few states have a security portal to coordinate IT and emergency-management responses across jurisdictional boundaries. We simply need a better approach for assessing risk, managing IT assets, reporting on security performance, setting architecture, and sharing resources. We also need a governance structure for IT that clearly defines roles and accountabilities.

The Scope of the Problem

Today there are 109.5 million Internet hosts on the World Wide Web. Five years ago there were 6.6 million hosts. Looking back only three years, there were 2.1 million high-level domain names. Today there are 29.9 million high-level names. Sixty-two percent of all U.S. households are now online. In the U.S. alone, 73.1 percent of all Internet users visit e-commerce sites.[2]

Just as the world is becoming more tightly interconnected via the Internet, the world is also accelerating IT automation with computers. For example, last year 7.4 million information appliances were shipped. By 2005, 51.8 million will ship annually. Even more staggering are the statistics on the shipment of personal computers. In 2000, over 49 million personal computers were shipped, and this will continue to increase dramatically each year for the next four years and beyond.[3] Parallel to these developments, a recent study by the National Governors' Association (NGA) reveals that this year states will spend $4 billion on homeland security.[4] A significant portion of this expenditure will go toward cyber-security. The Gartner Group reports that last year governments at all levels spent 6.4 percent of their revenues on IT. This spending level was 5.4 percent just a year earlier.[5] Clearly government has a strong commitment to digital government and IT infrastructure.

Digital government has many direct advantages for citizens and businesses. At the same time there are profound security risks and vulnerabilities, which must be managed. Digital government requires proactive IT governance and a robust infrastructure, which we know can be compromised by cyber-attacks, system failures, and natural disasters. If our electronic infrastructure is compromised at key points, the operations of government will be shut down with disastrous consequences. Recent global intrusions and virus attacks underscore this concern. The Code Red, Goner, and Qaz worms cost the private sector more than $13 billion in 2001.[6] Precise figures are not available for government specifically, but it is reasonable to assume that the costs are at least equal to that of private-sector organizations. It is very common for small- and medium-sized states to see 4,500 intrusion attempts per week.

Information Security magazine published the results of an October 2001 survey of 2,545 security specialists in both private and public-sector organizations. The following table shows the percentage of survey respondents reporting external as well as internal security breaches. The numbers speak volumes about the security risks to critical assets and the need for coordinated action.[7]

Table 1. Reported External and Internal Security Threats
Percentage of respondents experiencing these security breaches.

Category	2000	2001
Outsider/External Breaches	%	%
Virus/Trojans/Worms	80	89
Attacks on bugs in web servers	24	48
Denial of service	37	39
Buffer overflow attacks	24	32
Exploits related to active program scripting/mobile code	37	28
Attacks related to protocol weaknesses	26	23
Attacks related to insecure passwords	25	21
Insider/Internal Breaches	%	%
Installation/use of unauthorized software	76	78
Illegal or illicit use of computing resources (i.e., porn surfing, harassment)	63	60
Personal profit from computing resources (e.g., investing, e-commerce)	50	60
Abuse of computer access controls	58	56
Physical theft, sabotage, or intentional destruction of computing equipment	42	49
Installation/use of unauthorized hardware/peripherals	54	47
Electronic theft, sabotage, or wrongful disclosure of data or information	24	22
Fraud	13	9

Source: Reproduced with permission from Information Security.

Across our nation, thousands of technologists work tirelessly to discover, repair, and recover from the hundreds of attacks that penetrate IT infrastructures every day. We simply need a better approach.

A Holistic Approach

Security involves more than *just IT.* Holistic security is about physical security, disaster preparedness, emergency response, and critical infrastructure protection. Security requires multi-level cooperation and coordination of military, law enforcement, and subject-matter experts. Security touches auditors, facilities managers, and maintenance workers.

Security management begins with the adoption of security policies that have legitimacy within the enterprise. Security policies come from a process that builds consensus among many key stakeholders. This includes elected officials and other policy makers as well as end users, government employees, and citizens. Security policies should embody standard practices that everyone in the organization must follow. These standard practices include an understanding of specific outcomes or goals the enterprise is committed to achieve. These goals are critical to security planning and critical to assessments about how well the organization protects its assets.

Once security policies and standard practices have been agreed upon, the organization is ready to conduct a security risk assessment. The assessment documents the "as is" and compares the "as is" to the standard practices embodied in policies. The comparison yields a gap. Gaps are important because they point to initiatives. These "gap closing" initiatives are prioritized and become a part of the enterprise's long- as well as short-range security plans. After the initiatives are implemented, audits should be done to make sure the gaps are closed and the standard practices are followed. These audits also help organizations stay compliant to policies and standard practices. In addition, security audits and standard practices are key to creating IT enterprise security architectures. These architectures include design principles for building highly integrated and secure IT infrastructures and applications. Also, standard practices, audits, and security "gap" analysis are critical for establishing IT performance metrics. In fact, the best way to determine if security gaps have been closed and stay closed is through the use of metrics. Finally, intrusions and vulnerabilities should be closely monitored via automated and manual security technologies. Effective IT security cannot be managed with "guess-timates" or in an environment where responsible parties are too afraid to admit shortcomings. Once standard practices and metrics are in hand, the public-sector CIO is in a position to develop a compelling business case that points from the "as is" to the "to be" state of security, which will assure policy makers and stakeholders that security investments will be effective.

Many government systems provide essential services that touch citizens in a highly direct and personal way. These essential services are part of the nation's critical infrastructure. This makes IT security a key aspect of our nation's homeland security. Therefore, as metric data is gathered, it should be shared confidentially among the states and their federal partners. This will require a forum that fosters open sharing of case studies and lessons learned. We must develop a community of public-sector cyber-emergency responders to work with public safety, health, and emergency-management professionals.

Again, security done well is a way of life. For each of us to be secure, we must radically alter the way we live and the way we conduct our affairs. Radical—that is, fundamental—change is difficult because it challenges our traditional paradigms and our assumptions surrounding the way we live and work. Radical change for the ancient Greeks required a *metanoia*—a deep change of heart. September 11th made apparent the need to change our way of life, and the events of that day call us to a new epistemology—a *metanoia* that redefines what we mean by security and personal responsibility. Government leaders must set aside the "federated" cultures that foster agency autonomy and "my turf" thinking. We must share information, be more watchful, and become more disciplined in how we manage our affairs in community. We must also change our language about security. Security is more than "being safe." It is about justice and self-worth. It is about our dignity. Security is a way of life. This report will serve as a high-level guide for this new way of living.

Recommendations

MANAGEMENT

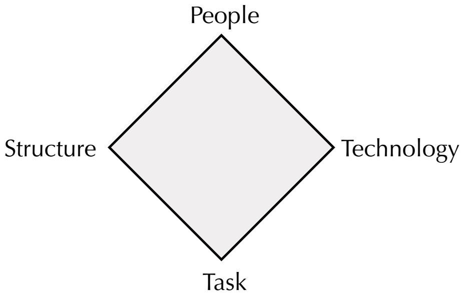
Recommendation 1: Implement an IT Governance Structure That Ensures Everyone Is at the Table

Develop an IT governance structure that is inclusive of all stakeholders. The structure should include security governance at the enterprise level and it should bring to the policy table emergency response and audit leadership. All branches of state government and local units of government should be represented in order to develop policies, set standards, and establish enterprise-level security plans.

Leavitt's Diamond

In 1965, Harold Leavitt, the Walter Kenneth Kilpatrick Professor of Organizational Behavior and Psychology (Emeritus) at Stanford University's Graduate School of Business, created a simple diamond graphic to depict the four key components of any organization.[8] Leavitt pointed out that all organizations are made up of people, structure, task, and technology.

Figure 1. Leavitt's Diamond



In 1994, Open Framework, a division of International Computers Limited of England, used Leavitt's Diamond to build a representation of how organizations exist within the context of their external social and technological environments.[9] Open Framework used this model to develop a highly popular methodology for enterprise IT architecture.

The Open Framework model defines "culture" to include individual roles and structure. The core values underpin management processes, which lay at the heart of organizational culture. CIOs live on the boundary line between the external and internal environment of the organization. On this boundary line, CIOs balance the four components of an organization against the constant pressures from the external social, economic, and political forces that

Figure 2. Open Framework Model

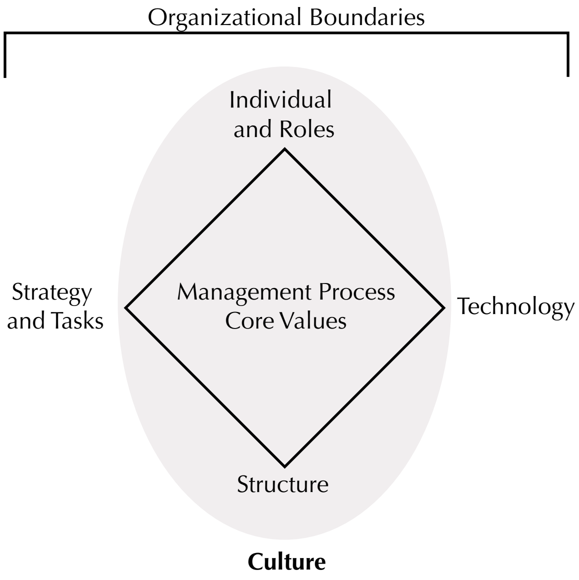
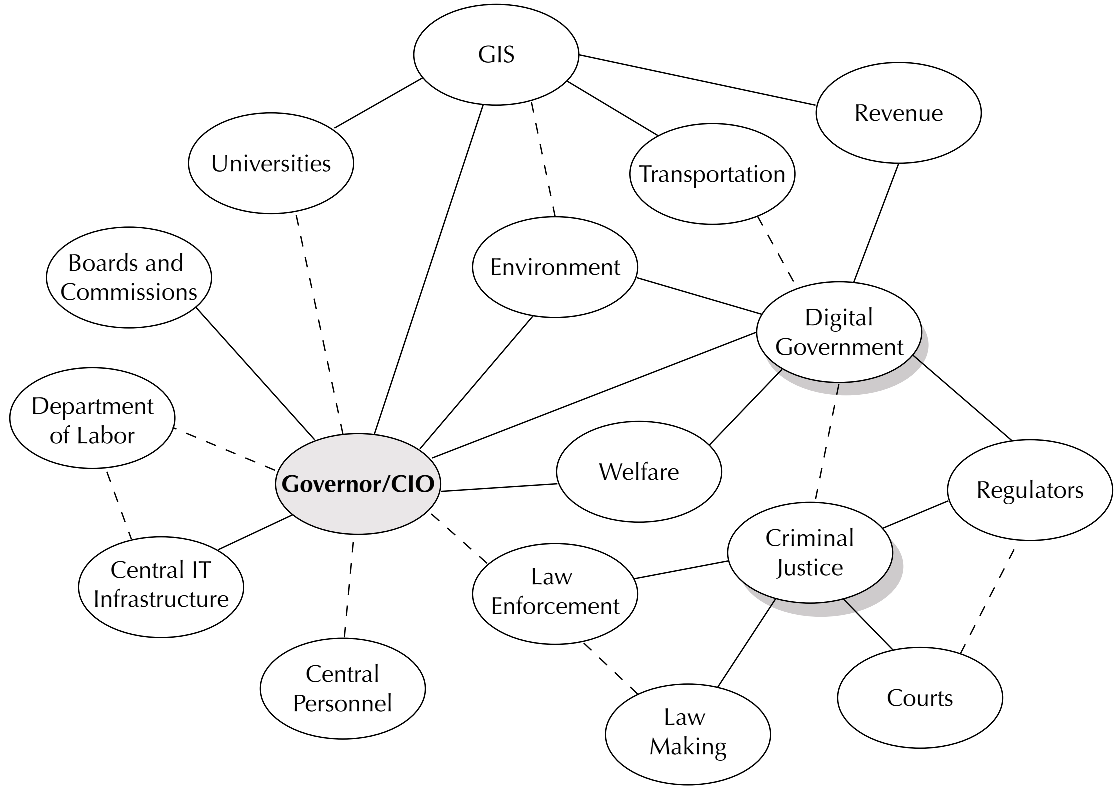


Figure 3. An Example of the Collegial Governance Arrangement



press on the enterprise. The Open Framework model also is designed to align management processes to business strategy and technology. The alignment occurs through structure and individual role responsibilities.

IT Governance Models

IT governance is critical to effective security policy making and implementation. In the U.S., public-sector IT governance arrangements reflect one of three distinctive patterns.

Collegial Model

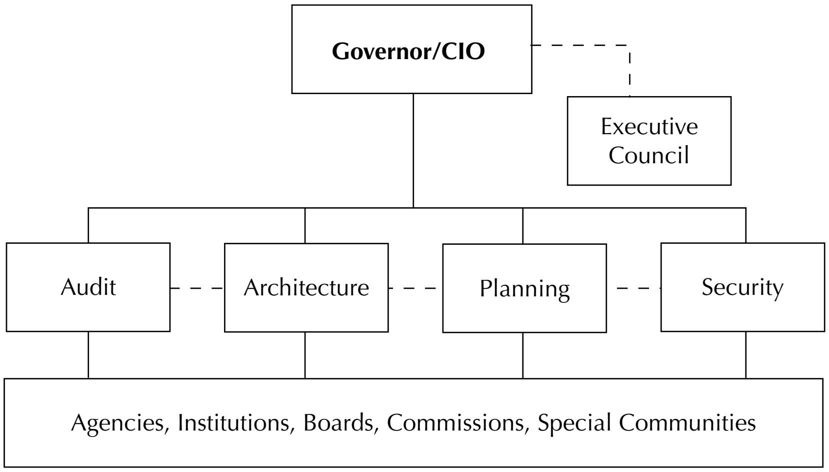
Many states use a CIO arrangement that could be described as "collegial." In this arrangement, the CIO reports directly to his or her governor and draws positional authority from the policy-making power of the governor and the cabinet. Collegial governance looks like a web with the CIO (and the governor) in the center and lines of influence and direction radiating outward toward agencies, commissions, and communities of interests. Since each state enterprise is uniquely structured, the lines of influence vary from state to state. Some lines are solid while others are dotted.

The collegial web grows over time, and the relationships—along with organizational affinities—change constantly. The CIO manages the context of IT through long-range planning, funding incentives, policies, and relationships. The CIO's staff is generally small but politically significant to the federation. Whenever there is a new governor or internal realignments (and conflicts) occur, the CIO, who relies on warm, professional relationships and reciprocal alliances throughout the enterprise, is at peril.

Rules-Based Arrangement

Almost as many states use a rules-based governance arrangement. These states have mature organizational linkages and laws, which come from active legislative oversight. Rules-based structures generally have an executive council, which performs primary oversight through approval reviews, policy making, standards setting, and planning. The CIO staff is larger than those found in collegial organizations. The rules-based CIO staff develops

Figure 4. An Example of a Rules-Based IT Governance Arrangement

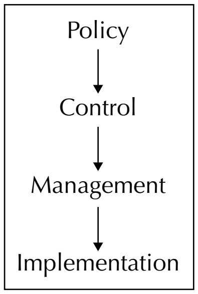

Governor/CIO
Executive Council
Audit
Architecture
Planning
Security
Agencies, Institutions, Boards, Commissions, Special Communities

enterprise reporting procedures, scorecards, and exception reports. The structure has a graduated, or hierarchical, structure. Rules-based structures are top down and rely on committees to achieve significant initiatives.

Often, rules-based structures do not cover all branches of government. Educational institutions, courts, and legislative oversight are more loosely coupled to the executive branch. In addition, concerns about separation of powers constrain the governance model because of the model's reliance on rules and exception reporting.

Roles-Based Arrangement

A growing number of states are moving toward a roles-based arrangement. This model follows the traditional hierarchy of an organizational structure.

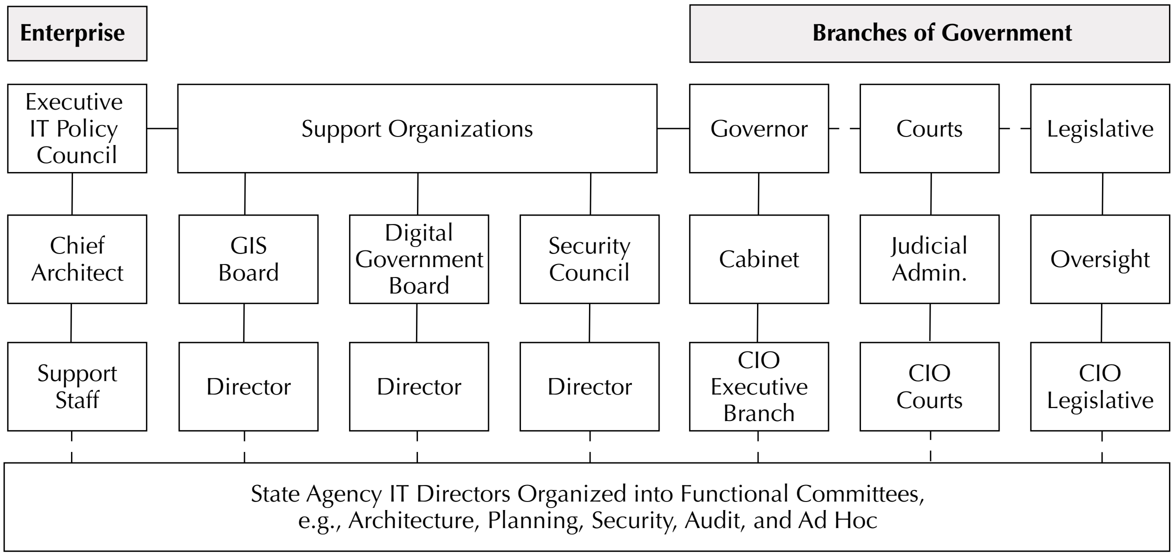


The policy role is high level and enterprise-wide in its focus. All branches of government are under the same enterprise policies while the individual branches of government retain their policy-making authority for the organizations and agencies under their jurisdiction. In order to strike a balance between the branches and the enterprise, the IT-governance statute must clearly specify the enterprise policy-making authority.

The roles-based model usually has a central executive council with broad-based representation. The representation includes all branches, educational leadership, local units, and private sector. The chief information technology architect for the state supports the council. The council is responsible for policies, long-range plans, project-management standards, and enterprise architecture. Enterprise security is also under the council's watchful eye. The governance model is modular in its design.

The state chief information technology architect, working with state agencies, prepares architectures, long-range plans, policies, and project management standards. The executive, legislative, and judicial branch CIOs manage and implement these enterprise plans, policies, and project management standards. The branch CIOs also approve projects, establish directions and plans influence funding, and implement architectures (for their branches of government). The branch CIOs are voting members of the enterprise executive council, and the executive-branch CIO sits in the governor's cabinet or occupies a similar cabinet-level position reporting to the governor. The support organizations depicted in Figure 5 work at the enterprise level as well as at the governmental-branch level.

Figure 5. An Example of a Roles-Based IT Governance Arrangement



[Note: In some states the executive branch CIO position might be a cabinet-level position or attached as an adjunct to the governor's office.]

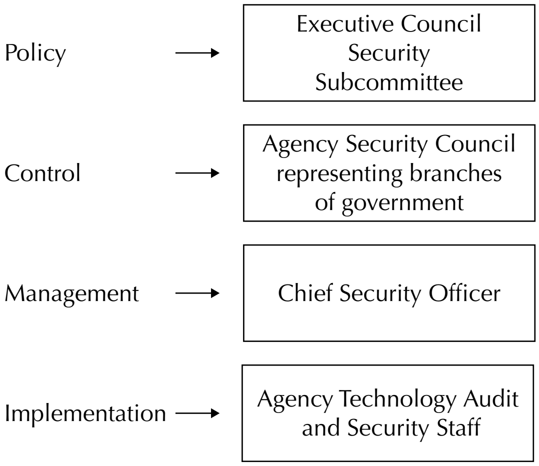
Security in a roles-based IT governance model is often handled through a subcommittee of the executive council for oversight. This subcommittee has policy authority over a security council representing all branches of government. The chief security officer reports to this council and draws staffing resources from the state agency-level IT directors. NASCIO's Enterprise Architecture Working Group has done some excellent research into roles-based governance, which is contained in its "Enterprise Architecture Development Kit, Version 1.0." The toolkit is available for free download at NASCIO's website at www.nascio.org/hotissues/ea.

The three governance models are rarely as pure as described here. Local, state, and federal governments use variants of each of the models. For this reason, a roles-based model may also use collegial- and rules-based substructures to achieve enterprise goals.

Despite the need for hybridized arrangements, local, state, and federal governments should create an IT governance model that allows the enterprise to set policies, standards, and practices for protecting critical infrastructures. At the state level, the IT governance model should include all the branches of government and clearly identify a security authority and an oversight body to monitor performance against policies and directions. All branches of government should subscribe to an enterprise architecture and shared infrastructure, project management standards, IT metrics, and audit standards for external and internal review of controls.

Finally, IT security must be integrated with emergency response at the state and local levels. State governments are uniquely postured to lead the integration because they are positioned between local units and the federal government. Also, the states' posture is enhanced with an IT infrastructure that

Figure 6. An Example of Security in a Roles-Based IT Governance Arrangement


Policy
Executive Council Security Subcommittee
Control
Agency Security Council representing branches of government
Management
Chief Security Officer
Implementation
Agency Technology Audit and Security Staff

touches cities, townships, counties, and other jurisdictions where people live and work. For this reason, state governments should realign their IT governance structure to fully involve local and federal government entities.

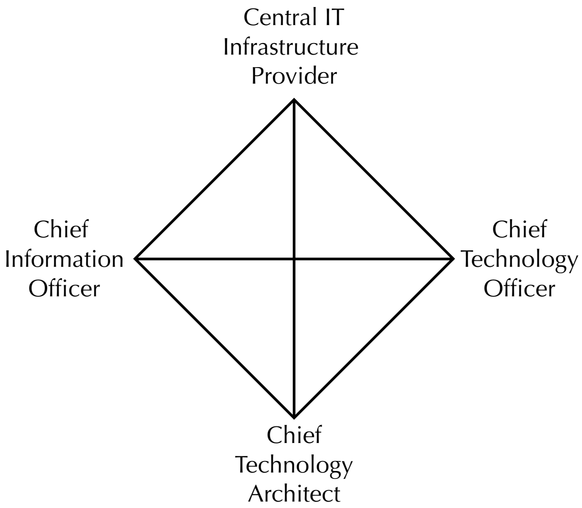
Recommendation 2: Implement Enterprise Planning for Outcomes to Measure Enterprise Success

Implement enterprise planning for outcomes, including measures for success and best practices for setting and performing tasks, and commit to sharing resources for the good of the whole.

People Are Key

Security relies on people, their expertise and their cooperation. In large government organizations there are many IT technologists as well as subject-matter experts who are IT literate and active in building systems. At any given period there can be 25 to 50 major IT systems under development. This is especially true for governments that are highly active in digital government initiatives.[10] Coordinating such a large and diverse labor force is very challenging for CIOs. Shared IT infrastructure and large application portfolios further complicate the challenge. In order to meet this challenge, CIOs seek to develop a coherent set of design principles, standard practices, and technology choices that are well grounded in the disciplines of information management. Moreover, a core team of at least four key players needs to be involved.

Figure 7. The Core Team



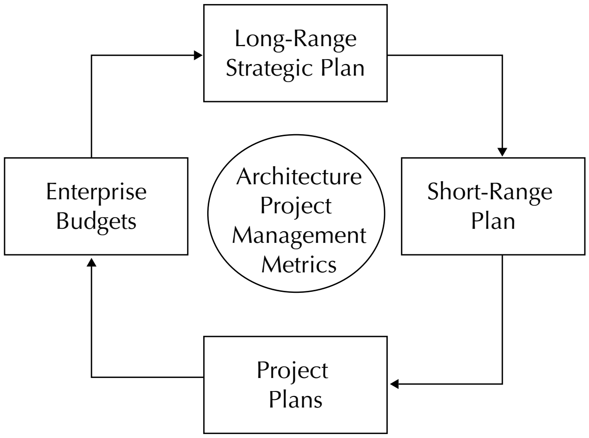
The CIO's job is more technical and managerial, while the CTO (chief technology officer) focuses more on the business case for IT. The central-infrastructure provider is technical and focused on shared resources, and the architect is focused on technical standards. Large government bodies have separate specialists for each of the four roles, while medium-sized organizations tend to combine roles. For example, medium-sized government organizations (i.e., 25,000 to 40,000 employees) might combine the CIO and CTO roles. Smaller jurisdictions could also benefit from combining the IT central infrastructure provider role with this position. As a general rule, it is best to keep the technology architect separate from the CIO role. This separation provides a check and balance. Here the architect plans and sets enterprise standards, while the CIO implements and manages to the architectures and standards. The two roles frequently overlap in the planning functions.

Enterprise Security Planning

Security Planning requires a clear understanding of enterprise plans and architecture and an understanding of IT technology and trends. The plans and architecture are based on guiding design principles, attributes, and standard practices and technologies that comprise the shared enterprise IT infrastructure. The guiding design principles must penetrate the organization in forming a "common will." The design principles form evaluation criteria and can be used as an enterprise "scorecard" against which to measure successes and set initiatives. Clearly the workforce must be properly trained in these guiding design principles, standard practices, and the technologies that comprise the shared enterprise IT infrastructure. Communication and Coordination are key aspects of Enterprise Security Planning.

Strategic long-range plans set priorities for the enterprise. When determining enterprise priorities, it is essential to include stakeholders. Leveraging expertise of many participants to understand unique requirements and constraints can result in "win-win" shared IT infrastructure choices. Figure 8 depicts the Planning Cycle showing the relationship between enterprise long-range planning, short-range planning, projects, enterprise budgets, and shared enterprise architecture and infrastructure. Security planning is part of this overall planning cycle.

Figure 8. The Planning Cycle


Long-Range Strategic Plan
Short-Range Plan
Project Plans
Enterprise Budgets
Architecture Project Management Metrics

The planning model above moves from strategy in long-range and short-range plans to tactics in individual project plans and enterprise budgeting. Enterprise Architecture drives and supports formation of an enterprise infrastructure. Project management, and metrics are crucial to measuring success of individual projects for both conformance to the enterprise architecture and infrastructure as well as contributing to the evolution of the enterprise architecture and shared infrastructure. Security is addressed as a sub-architecture and in the metrics used to measure progress. The security gaps identified in this process are addressed in project plans and budget considerations.

Recommendation 3: Adopt IT Control Objectives

Adopt IT control objectives to manage, implement, and maintain IT systems.

COBIT®[11]

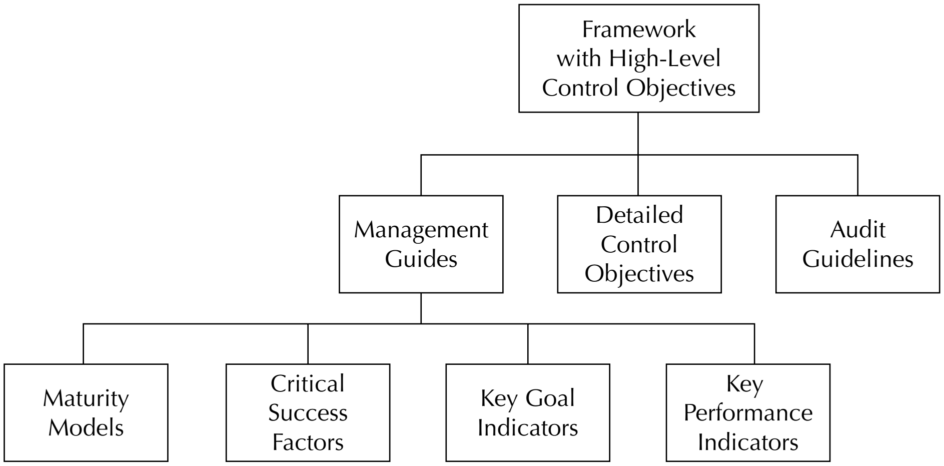
Developed by the IT Governance Institute and the Information Systems Audit and Control Association and Foundation (ISACA/ISACF), COBIT—Control Objectives for Information and Related Technologies—provides a framework designed to assess how well internal controls support the business processes and requirements of the enterprise. The objectives cover information technology effectiveness, compliance, integrity, and efficiency. The standards also address key planning and organizing practices, acquisition and implementation of IT resources, delivery and support, and monitoring performance against standards. The COBIT "Executive Summary" consists of an Executive Overview that provides a thorough awareness and understanding of COBIT's key concepts and principles for management awareness.

At the heart of the COBIT framework are assessment instruments for evaluating application systems, technologies, facilities, data, and people. The COBIT framework, which explains how IT processes deliver the information that the business needs to achieve its objectives, divides IT into 34 high-level control objectives, one for each of 34 IT processes, contained in four domains as follows:

- **Planning and Organization**—covers strategy and tactics, and concerns the identification of the ways IT can best contribute to the achievement of the business objectives.
- **Acquiring and Implementing**—deals with identifying IT solutions as well as implementing and integrating them into the business process. Life-cycle issues such as changes and maintenance of existing systems are also covered by this domain.
- **Delivery and Support**—addresses the delivery of required services, ranging from traditional operations over security and continuity aspects to training. This domain also includes the actual processing of data by application systems.
- **Monitoring**—guides management's oversight of the organization's control process and independent assurance provided by internal and external audits, as IT processes must be regularly assessed for their quality and compliance with control requirements.

The framework also takes into account fiduciary, quality, and security needs for the enterprise and provides for seven information criteria (i.e., effectiveness, efficiency, availability, integrity, confidentiality, compliance, and reliability) that can be used to generically define what the business requires from IT as well as which IT resources (i.e., people, applications, technology, facilities, and data) are impacted. In addition, 318 detailed control objectives have been established for IT management and practices.[12] Also, CobiT contains audit guidelines that provide suggested audit steps corresponding to each of the 34 high-level control objectives.

Figure 9. Hierarchy of CobiT Framework Materials


Framework with High-Level Control Objectives
Management Guides
Detailed Control Objectives
Audit Guidelines
Maturity Models
Critical Success Factors
Key Goal Indicators
Key Performance Indicators

Source: Reprinted with permission of ISACA.

As shown in Figure 9, the Management Guides are composed of the following:

- **Maturity Models**—to help determine the stages and expectation levels of control and compare them against industry norms.
- **Critical Success Factors**—to identify the most important actions for achieving control over the IT processes.
- **Key Goal Indicators**—to define target levels of performance.
- **Key Performance Indicators**—to measure whether an IT control process is meeting its objective.

These Management Guidelines help answer the questions of immediate concern to all those who have a stake in enterprise success.

CobiT was founded in the belief that successful enterprises, such as states, must manage the effective union between business processes and information systems.[13] The model depicts central functions as a driver of enterprise activities. The controls help ensure that business objectives are met through vigilance to best practices and effective as well as efficient use of resources. CobiT emphasizes security and helps the organization better control the task dimension of Leavitt's Diamond.

FISCAM

Some states use the "Federal Information Systems Control Audit Manual: Volume I Financial Statement Audits" (FISCAM) developed by the U.S. General Accounting Office (GAO). The body of standards presented in the manual "…provides auditors guidance in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems,"[14] (FISCAM cites COBIT as a key reference in each of its sections addressing evaluating and testing of these controls.) It takes an enterprise perspective and can be used to integrate IT architecture, governance, and planning activities across all branches of state government. It also ties in nicely with a number of key federal directives and initiatives to include:

- Presidential Decision Directive 63: "Protecting America's Critical Infrastructures" at www.fas.org/irp/offdocs/pdd-63.htm
- Presidential Decision Directive 67: "Enduring Constitutional Government and Continuity of Government" at www.fas.org/irp/offdocs/pdd/pdd-67.htm
- NIST Special Bulletin 800-14: "Generally Accepted Principles and Practices for Security of Information Technology Systems"at http://csrc.nist.gov/publications/nistpubs/ (See "SP 800-14.")

- NIST Special Bulletin 800-18: "Guide for Developing Security Plans for Information Technology Systems" http://csrc.nist.gov/publications/nistpubs/ (See "SP 800-18.")
- NIST Special Bulletin 800-26: "Security Self-Assessment Guide for Information Technology Systems" http://csrc.nist.gov/publications/nistpubs/ (See "SP 800-26.")
- NIST Special Bulletin 800-34: "Contingency Planning Guide for Information Technology Systems" http://csrc.nist.gov/publications/nistpubs/ (See "SP 800-34.")

The GAO and the National State Auditors Association (NSAA) have jointly published a companion manual, the Management Planning Guide for Information Systems Security Auditing (www.gao.gov/special.pubs/mgmtpln.pdf) to help organizations implement FISCAM reviews. (See GAO's "Special Publications: Computer and Information Technology" web page at www.gao.gov/special.pubs/cit.html for more information, including "Federal Information System Controls Audit Manual: Volume I Financial Statement Audits," "Information Security Risk Assessment: Practices of Leading Organizations," and "Information Technology: An Audit Guide for Assessing Acquisition Risk.")

Many public- and private-sector organizations provide assurance services, including security reviews, control assessments, and policy guidance. These organizations include the Centers for Medicaid and Medicare Services (CMS) (http://cms.hhs.gov) and the American Institute of Certified Public Accountants' (AICPA) SysTrust (www.aicpa.org/assurance/systrust/princip.htm), just to name a few.

Recommendation 4: Develop Security Metrics

Develop security metrics that accurately measure unwanted intrusions, security breaches, penetrations, and vulnerabilities. The reporting should be shared at a summary level with the executive, legislative, and judicial branches of state government as well as with other governmental organizations. The reports should be confidential to government communities.

In order for security to permeate the plans and culture of an organization, the CIO needs to develop a set of reporting metrics that clearly show whether security requirements are being satisfied. The metrics flow from several important sources.

Audit Findings

Internal and external auditors evaluate general and application controls in order to determine the level of test work required to confirm the accuracy and reliability of financial statements. Audits identify weaknesses in management practices and in security. Auditors, who evaluate specific controls related to IT systems and security, are a rich source of information for CIOs, IT infrastructure providers, chief security officers, and chief technology officers, as well as technology architects.

Intrusion Attempts and Penetrations

IT security officers are very interested in the count of intrusions that appear in scanning reports, as well as penetration counts, the level of penetrations, and the nature of the penetrations. Finally, security officers are highly sensitive to the count of attacks that come from internal as well as external sources. This information should be gathered at the department level of the organization and reported at the enterprise level through the CIO and into the IT governance structure.

Virus Alerts and Recovery

A constant readiness center, intrusion response team, or an equivalent must know when viruses infiltrate the organization, how the viruses negotiated their way through security, and the resources used—measured in elapsed time and cost—to recover from the viruses. Distributed denial of service (dDoS) attacks, viruses, worms, hacks, sloppy users, breaches of physical security, and software failures are part of the normal conduct of business. The important point here is that CIOs know when these events are increasing beyond a baseline. Also, it is very important that the CIO knows what caused the spike. Basic systems should have 99.9 percent ("three nines") availability. However, mission-critical systems require an availability baseline as high as 99.999 percent ("five nines"). This higher level is required in mission-critical criminal justice, payment, and payroll applications, to mention only a few. When availability drops below these levels, the CIO must be informed.

National Alerts

National alerts are important sources of information for CIOs and chief security officers. There are many national organizations that report alerts and provide subscriber services to customers who need technical help to protect core systems or processes. NASCIO's Security and Reliability Team assembled the following descriptions of some of the many IT security resources that operate on a national and international scale and are available to all public-sector CIOs and security chiefs.

- **CERT/CC**
  The Software Engineering Institute (SEI) at Carnegie-Mellon University established the CERT/CC in 1988. SEI is a federally funded research and development center with a broad charter to improve the practice of software engineering. It is also an excellent source for incident statistics. (www.cert.org/nav/index.html)
- **National Infrastructure Protection Center (NIPC)**
  An operational entity of the FBI, NIPC serves as a national critical infrastructure threat assessment, warning, vulnerability, and law-enforcement investigation and response entity. It is an excellent source for critical alerts emanating from the federal government. (www.nipc.gov)
- **Critical Infrastructure Assurance Office (CIAO)**
  An agency of the U.S. Department of Commerce, CIAO was created in response to Presidential Decision Directive 63 (PDD-63) in May 1998. CIAO assists states and local units of government on critical infrastructure protection strategies. Their services are also available to industry sectors. (www.ciao.gov)
- **Partnership for Critical Information Security (PCIS)**
  Also originating from PDD-63, PCIS is a non-profit entity providing public-private collaboration. It operates out of the U.S. Chamber of Commerce. (CIAO leads federal government participation in PCIS activities.) It coordinates outreach to the eight national critical infrastructure sectors, which include information and communications, electric energy, gas/oil production and storage, banking and finance, transportation, water supply, emergency services, and government services. PCIS also addresses sector interdependencies, vulnerabilities, information sharing, and public awareness. (www.pcis.org)
- **System Administration, Networking and Security Institute (SANS)**
  Founded in 1989, SANS is a cooperative research and education organization of system administrators, security professionals, and network administrators. The institute is a unique partnership of government agencies, private corporations, and universities from around the world. It is also an excellent source for vulnerability reports and global trends in cyber-threats. (www.sans.org/newlook/home.php)
- **National State Geographic Information Council (NSGIC)**
  Members of NSGIC include senior geographic information system (GIS) managers representing state government, federal agencies, local government, the private sector, and education. The association provides research, best practices information, and technical training, including uses of GIS for homeland security. (www.nsgic.org)

Intra-State Security Information Sharing and Analysis Centers

Many state, federal, and local units of government rely on the organizations profiled above. However, the resources of these organizations alone are not targeted enough to effectively handle the growing incidents of intrusions, viruses, and hacks seen by a particular enterprise. As a result, a number of states have developed internal security information sharing and analysis centers or ISACs, to help their security officers analyze and parse intrusions. These *intra-state* ISACs are frequently linked to a constant readiness center, which is the coordinating center for state government enterprise response and recovery.

Some intra-state ISACs consist of inter-agency list-servs that allow a state's security chief to push alerts to the agency IT directors. They also allow the list membership to collectively analyze incidents and suggest responses. As they mature, intrastate ISACs will be staffed with specialists who have expertise in hardware, software, networks, and physical security. The ISACs will also have emergency response specialists trained in emergency management disciplines and well versed in techniques for IT disaster preparedness and recovery. ISAC specialists will work side by side with certified IT disaster recovery experts. In addition, the ISAC's staff should be trained in audit standards such as those in the IT Governance Institute's CobiT (Control Objectives for Information and Related Technologies) or the U.S. General Accounting Office's Federal Information System Controls Audit Manual (FISCAM), depending on that state's audit approach. Also, they should be familiar with generally accepted security standards such as ISO/IEC 17799 ("Code of practice for information security management").

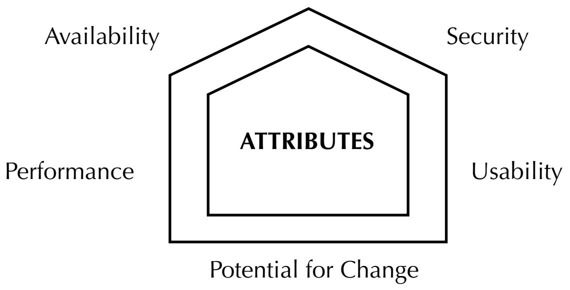
Recommendation 5: Develop Enterprise-IT Security Architectures and Establish a Shared/Common Security Technology Infrastructure

Develop state enterprise-IT architectures using accepted architecture-setting methodologies. Define the security domain of the architecture based on guiding design principles and standard practices. Establish an enterprise shared infrastructure by defining a common set of technologies and approaches that can be leveraged across the enterprise.

Stephen Covey says that effectiveness begins with the "end in mind."[15] The "ends" for organizations are commonly referred to as "goals." Five key qualities should be considered when decisions are made about system goals and their effectiveness. The system must have:

- Potential for change
- High availability
- High usability
- Adequate performance
- Reliable security (i.e., trustworthiness)

Figure 10. System Architecture Qualities



Each of these five qualities must be in balance. For example, security affects system availability, and it can also degrade performance and usability. It is a tradeoff. As systems become more difficult to access, the usability of the system will decrease. Security also adds overhead to the system, which in turn adversely affects performance. The tradeoffs require an understanding of risks, user/stakeholder needs, current costs, staff skills, and the business demands for each system. These business demands, which can be categorized by attribute, are key. They drive total cost of ownership and determine staffing skills required to balance the tradeoffs. Table 2 presents key factors related to each attribute.

These attributes flow through the business, application, information, and technical architectures. They permeate the sub-architectures that describe information technology from different perspectives—from the point of view of the application developer, end user, service provider, and IT manager. Many specialists are involved and their perspectives are critical to system integrity, reliability, and, ultimately, performance. Again, security, a key architectural component, is about people and how well they are able to blend perspectives and talents.

Recommendation 6: Develop a Business Case for Security

Develop a business case for security. The business case should be based on a full risk assessment of critical-infrastructure vulnerabilities. The risk assessment should include a complete inventory of critical systems and assets. The assessment also should

Table 2. Business Demands Attributes

Availability	Usability	Performance	Security
Reliable components Error detection Fault tolerance Repair Preventive maintenance Distribution, installation, and activation	User testing and evaluation Requirements capture and analysis Ergonomics Consistent user interface Support services, training, and documentation	System predictability Comparability and benchmarks Manageability, control, and monitoring	Confidentiality Integrity Availability to authorized users Accountability Non-repudiation

involve a gap analysis between actual and ideal security levels for the identified systems and assets.

It is natural to ask: "How do I begin building a secure environment?" As mentioned earlier, Covey reminds us "to begin with the ends in mind."[16] The ends he refers to are the targets we want to hit. Risk assessment helps us define the targets for a secure environment. Risk assessment also helps us know where we stand today. The following recommendations outline a simple approach that can be used to perform risk assessments. The approach has a start-up phase and five follow-on steps.

Step 1. Determine Actual "As Is" Risk

There are many risk-assessment methodologies. However, the best methodologies share a core logic that starts with an inventory, determines criticality, and analyzes the number of people affected if a given asset is lost. These three processes are used to create an Impact-Risk Index. Next, the analysis examines the time required to recover if the asset is lost. This information is also indexed and multiplied by an estimate of the probability of losing an asset. This is called the Recovery-Loss Index. An actual risk assessment index is then calculated by multiplying the Impact-Risk Index by the Recovery-Loss Index. The result is an Actual Risk Index expressed as a percentage.

Impact-Risk Index x Recovery-Loss Index = Actual Risk Index

Step 2. Determine the Target or "To Be" Risk Index

The security council and asset owners should meet and, using the most reliable data available, develop a target risk index acceptable to the enterprise. The target risk index is expressed as a percentage. Some assets with low criticality might have a high target-index number, such as 10 percent, while highly critical assets might have a low target-index number, such as 1 percent. The target index represents the amount of risk an organization is willing to accept against various types of cyber-threats. When the index is high, more risk is accepted; a low index number means only minimal risk is acceptable.

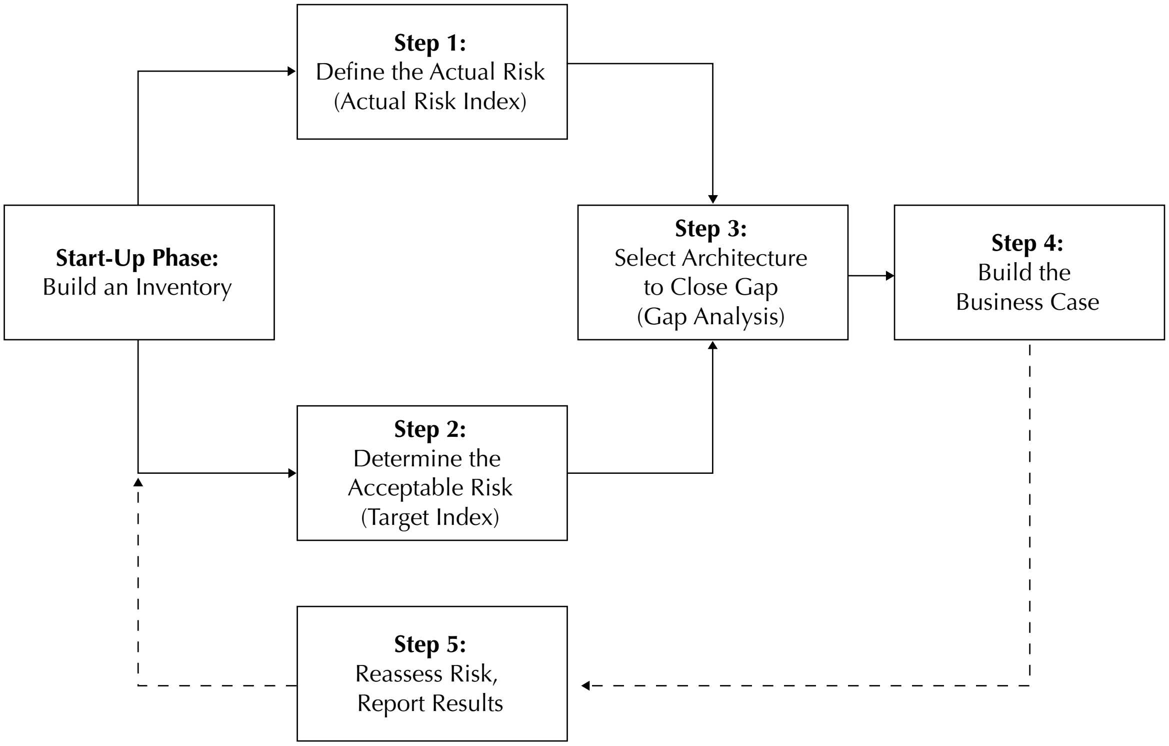
Step 3. Determine and Close the "Gap"

Risk assessment methodologies also include gap analysis. The analysis compares the acceptable risk ("to be") with the actual risk level ("as is"). The difference is called the "gap." It is oftentimes expressed as a positive or negative percentage. Negative gaps indicate the enterprise is at risk, while positive gaps mean security for an asset meets or exceeds expectations.

Acceptable Risk Index - Actual Risk Index = Risk "Gap"

In addition, popular methodologies include a process for closing the gap. This process uses the enterprise architecture to select security sub-assembly

Figure 11. Simplified Risk Assessment



architectures that best fit the criticality and recovery time for the asset or system. The goal is to select a security architecture that produces a positive "gap" score.

Step 4. Build the Business Case

The fourth step in risk assessment involves building the business case for security. The security council and asset owners should estimate the cost for the security architecture selected to reduce the gap. This cost is compared to economic and qualitative losses if the security architecture is not implemented. This represents a cost-avoidance benefit and is central to determining the feasibility for implementing security initiatives. This benefit is called an exposure to loss reduction.

Step 5. Implement, Reassess, and Report Results

The last step is often not done, yet it is the most important. Security is organic in the sense that security must adapt to changing conditions caused by technology advances as well as changing threats upon the enterprise. For example, the events of September 11, 2001, dramatically changed the exposures to loss and the probabilities that affect security indices. Such events also drive innovations in architecture. For these reasons, the security council needs to evaluate the implementation of new security initiatives on at least a quarterly schedule. These evaluations involve refreshing the risk assessment and reporting the results to asset owners and to the IT governance authority. Finally, CIOs should make sure all security initiatives comply with change management disciplines and that the inventory of assets is updated to reflect security architectures and current risk assessments.

The inventory is more than a listing of assets and systems. The inventory should include an estimate of the number of people affected by the systems along with the risk assessment for "as is" and "to be" risks. Also, the inventory should properly report the "gap" index for each asset or system.

TECHNOLOGY

Recommendation 7: Deploy Security Technologies

Define security controls and deploy automated and manual security technologies based on asset inventories and application criticality, including security levels derived from the enterprise architecture for IT.

The following recommendation covers methods organizations use to select appropriate security technologies. In the following example, IT security architectures are grouped into three levels. The choice of a security level to protect an asset depends on the asset's importance, vulnerability, and value. There must be a current and accurate inventory of IT assets to drive the security-level selection process.

Level 1—Basic

This lowest level contains the minimum architecture for security. Basic security includes control over physical access to data centers and enterprise networks. Documented entry systems such as keycard entry and log reports are required for physical access to the data center and other secure areas. Also, passwords are required for electronic access to IT systems. Passwords should be at least nine characters with capital and lowercase letters, numbers, and symbols. Software should be able to deny password changes that repeat or are closely related to historic passwords used by individuals. Password changes should be forced every two to four weeks. Finally, network scans and virus protection disciplines are critical to basic security practices.

Basic security also requires a complete understanding of LAN segments. The understanding includes server placement as well as application assignments on the LAN segments. In addition, firewalls and basic encryption using a Secure Sockets Layer (SSL) are required. Applications should also have password protection and forced-change procedures as mentioned above. Finally, the applications should have a full array of edits, exception reporting, check digits, and balance confirmations like batch-control totals and transaction controls. Confirmation of application controls is the independent responsibility of functional users who own the application. Here separation of duties is very important.

Basic security also requires frequent reviews of system logs, strong controls over administrator rights, and a robust procedure to manage system-level patches, fixes, and emergency upgrades. Technical support owns the system-level software and the security process to properly control deep system-level changes, such as those to operating systems or utilities.

In order for general and application controls to exist, three criteria must be satisfied. First, control must first be established. Second, it must operate. And, third, the operation must be supervised through independent confirmation by management. If any of these three requirements is missing, control—by definition—does not exist. Finally, basic security requires control over system-level changes and application changes. These changes must be subject to version control, documentation, and recovery disciplines. Change management is fundamental to security.

Level 2—Medium

The medium level of security requires an architecture that emphasizes complete authentication of those who access IT systems. The authentication can include public key infrastructure (PKI), biometrics, cryptographic-card technology, or variants thereof that confirm that a given user is, in fact, the person whom he or she claims to be. Also, callback technologies are frequently used to confirm that certain devices are authorized to access certain networks.

For mission-critical applications, managers are responsible for passwords that are used to perform emergency fixes. These passwords are kept in sealed envelopes under lock and key. They can be used only once. All passwords are encrypted using at least 256-bit encryption algorithms. Finally, users are barred from a system after two failed attempts to properly enter the correct password and/or user identity. All exceptions are logged and independently reviewed by system administrators as well as system owners.

Cryptographic-card technologies allow users to have unique passwords for each session. This technology is frequently used in law enforcement applications. The password exists only for enough time to allow log-on. Also, the passwords are fully encrypted and security administrators closely monitor the use of the cards. More sophisticated network scans, transaction sheathing (such as tunneling technologies), and request-callback techniques are also used to secure systems that require medium-level security. Finally, critical data that passes through networks at this level should be fully encrypted.

Level 3—High

This highest security level moves from defense to offense. The network should know who is seeking access to a given system and sound the alarm when unauthorized access is attempted or gained. Knowledge of the user is ascertained by full authentication, confirmation based on application security profiles, and full authorization.

The highest level of security also includes active system scanning, random "white hat" hack attempts by security officers and auditors, and masking of infrastructure through the use of "honey pots" that entice hackers to false targets where they can be monitored and "tar pits" that bog down the spread of viruses and worms within a system. Security technologists use tar-pit logs to reverse-engineer attacks and to trace the identity and source of intrusions. Finally, security officers notify organizational partners when that partner's infrastructure has been compromised, thus exposing the state's systems. Security officers work closely with law enforcement and, with help from the legal staff, are empowered to press legal charges against those who attempt to compromise systems.

Organizations must have policies for monitoring unauthorized installation of software by employees in violation of security protocols and license agreements. System administrators should frequently examine the software operating on PCs and servers to confirm that the software is appropriate and that software versions conform to organizational standards. Also, security officers and local campus administrators must have current procedures for responding to virus attacks. The procedures should give the officers and administrators the authority to disconnect devices that threaten the stability of LANs, metropolitan area networks (MANs), and wide area networks (WANs). Security is not for the fainthearted; it is hard work and it has costs. As mentioned earlier, regardless of level, effective controls exist when three criteria are satisfied. First, control must be established. Second, it must operate, and, third, the operation must be supervised through independent confirmation by management. If any of these three requirements are missing, control—by definition—does not exist.

Recommendation 8: Develop A State Security Portal

Develop a state security portal that integrates with emerging technologies for emergency responders such as intelligent roads and radio-frequency infrastructure. The state security portal should have a public access site as well as a private, enterprise site for coordinating emergency response.

Earlier we discussed the key people involved in setting enterprise standards. Remember the core team graphic.

These four positions form the core team for setting enterprise design principles, standard practices, and technology choices for the shared enterprise infrastructure. However, the core team requires help to develop security sub-architectures. For this reason, the core team needs to add emergency response team specialists. These specialists include the chief security officer and the director of the constant readiness center.

Figure 12. The Core Team (Revisited)

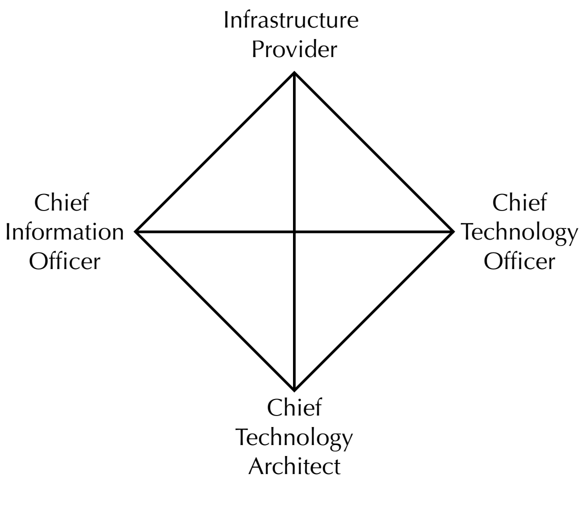
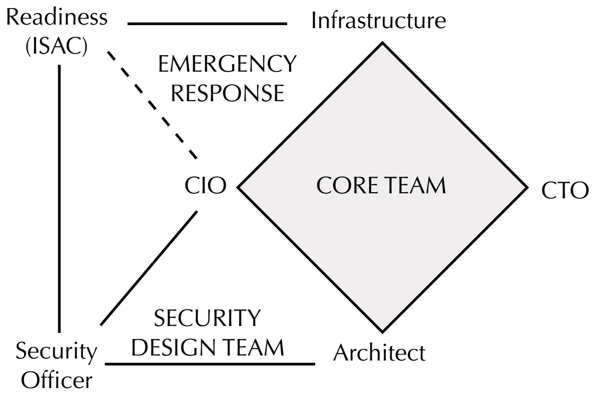


Figure 13. The Expanded Core Team



Also the core team should include a security design team to assist those who manage the constant readiness centers and ISACs. This computer emergency/incident response team (CERT or CIRT) should include the state CIO, director of the readiness center/ISAC, chief security officer, and the director(s) of the shared data center and network infrastructures. The CIO is the linchpin for core, design, and response teams.

In addition to managing emergency response, the CERT is responsible for managing a security portal used by the enterprise, citizens, and businesses that rely on state services. The portal has a secure as well as public access site. The portal should be designed to help emergency management notify and assist citizens in time of crisis. It should also help coordinate the enterprise's response to disasters and major security breaches. The portal site relies heavily on geographic information system (GIS) technologies. GIS is a key technology for integrating security response and applications that support these responses.

The portal provides controlled private access to applications that include 511-truck routing, ambulance responses, 911 services, criminal-justice information-system alerts, and Federal Emergency Management Agency (FEMA) response. The public security portal also includes placeholders to report critical infrastructure alerts such as water contamination sites, power failure locations, road closings, fires, and telecom outage areas. The site also shows civil defense facilities, schools, hospitals, and related support service locations critical at the time to emergency response. The secure site is designed to push critical-infrastructure information, including maps locating assets valuable to law enforcement and emergency management personnel. The portal should also be designed to coordinate FEMA response teams, the National Guard, and IT specialists.

In its most sophisticated form, the security portal is more than a website. The portal should be tied to intelligent highway systems to include electronic signs and disparate emergency radio broadcast frequencies. Citizens should be able to view critical-infrastructure messaging from roadside electronic billboards and hear these messages on home and car radios. True integration is more than a web page and requires leveraging common enterprise infrastructure to full benefit.

HOMELAND SECURITY

Recommendation 9: Establish an Interstate ISAC

Establish an interstate security information sharing and analysis center (interstate ISAC) funded at least partially by the federal government. The interstate ISAC, building on the federal-sector ISAC model, will assist states in analyzing security breaches, repairing affected systems, reporting security alerts, providing clearinghouse services for progressive practices, and interfacing with appropriate federal entities.

Many states will not have the resources to staff and fund their own intrastate ISAC. States realize that the cost of these services is high and the level of talent required to unravel hacks is difficult to find. It takes highly specialized skills to handle a hack in deep infrastructure. An *interstate* security information sharing and analysis center (interstate ISAC), built on the federal-sector ISAC model, could provide these skills and aggregate state incident data to support national strategic cyber-security planning. NASCIO should continue its effort to answer the recent call by Howard Schmidt, vice chairman of the President's Critical Infrastructure Protection Board, to coordinate the creation of an interstate ISAC to supplement individual states' efforts.[17]

Also, the interstate ISAC could help states coordinate their responses to cyber-attacks and serve as a liaison to law enforcement and national defense entities. Coordination also includes dissemination of best practices for meeting audit exceptions and for implementing security standards promulgated by oversight bodies, internal auditors, and federal agencies that have issued mandates such as the Health Information Portability and Accessibility Act (HIPAA) security rules. As with intrastate ISACs, an interstate ISAC must have staff trained in generally accepted audit and security standards. These standards cover basic disciplines for how states manage IT resources. The standards also establish a context for setting security architectures and initiatives.

The interstate ISAC will:

- Assist states and local units in their efforts to thwart unwanted penetrations
- Identify sources of attacks
- Help in repairing affected systems
- Scan for unwanted intrusions
- Develop strategies and tactics for being more offensive in protecting systems and critical infrastructure, including IT strategies for identifying and prosecuting perpetrators
- Advise on security architecture
- Serve as a clearinghouse of high-level information and statistics about security risks and violations
- Provide early warning and notice
- Partner with laboratories and corporations for testing new technologies such as honey pots and tar pits for deployment in the states

Recommendation 10: Develop Model State Legislation for Information Sharing

Develop model state legislation that allows local, state, and federal entities to confidentially share security incident reports among themselves and with other ISACs supporting the nation's critical-infrastructure owners and operators.

In order to coordinate response, understand critical infrastructure, develop national strategies, and disseminate best practices in cyber-security, governments must share sensitive security information among themselves. However, this information can be a powerful weapon in the wrong hands. For this reason, sharing will not occur unless there is an assurance of confidentiality against state open records/sunshine laws and the federal Freedom of Information Act (FOIA). Interstate sharing has been limited because states fear that their security activities could become a part of another state's open records when information is shared across state boundary lines or with local or federal units of government. Also, it is difficult for CIOs to coordinate the sharing of security information that is highly sensitive to an agency, board, or commission. Nonetheless, coordination and sharing information is crucial to protecting critical infrastructure. Legislation is required at the state and national levels to provide the necessary assurances that intergovernmental security reports will be held in confidence. Security, privacy, and open records must be in balance. Finally, the legislation should prohibit private-sector firms from disclosing sensitive security information acquired in the normal course of business with governments.

Conclusions

Security is a tough business. It is intellectually challenging and emotionally draining. It is simply wrong to place the burden of security solely on the shoulders of security officers, technologists, and IT executives. Security is a shared responsibility across the entire enterprise, to include subject-matter experts, functional users, and oversight professionals. Secure organizations are built on a culture that is open, resource sharing, and focused. Secure organizations do not happen by accident.

For security to be effective, governments should teach all their employees control standards and build the standard practices into their planning and measuring processes. They should provide clear feedback through audit reports and metrics to confirm that security is properly practiced. Good security comes from a highly trained and motivated workforce. In his theories about motivation, Vic Vroom, John G. Searle Professor of Organization and Management at Yale University, created a simple model about what drives individual and corporate behavior. He said people must know what is expected. They also need to know how to meet the expectations. Armed with this knowledge, employees need to understand rewards and actually value the rewards. Finally, this knowledge must come from direct and fair feedback. Vroom said that if any of those key ingredients are missing, then motivation to act breaks down.[18] Vroom's theories are as valid today as ever.

Our children want a world that is more advanced and, at the same time, more "user friendly" than the one we have today. They want an online world that is less bureaucratic and more "life-event" driven. In this world, online government information and services are organized around significant events such as getting married, obtaining a driver's license, opening a business, coping with the loss of a loved one, or responding to a public emergency. They want a world that is "one stop" with "no wrong door." In that world the boundary lines of government will be seamless. In essence, our children want a virtual government—meaning anything done in the presence of government can be done electronically without regard to time and location. Security in that world will be non-intrusive, reliable, confidential, and available. Security in that world is tailored to the needs of citizens and businesses.

There is an epistemology—that is, specific theories and knowledge—that underlies security and IT. It is soulful—deeply personal, virtuous, and mindful of others' needs. This report calls public-sector CIOs to take up this epistemology. It calls for a metanoia that radically changes the way governments interact by creating new ways to share resources in order to protect vital interests. CIOs are called to develop IT governance structures that are open, sharing, and highly secure. They should follow Vic Vroom's advice about motivation, clearly plan security outcomes, teach security best practices, build security responsibilities into all position descriptions, provide feedback though metrics and scorecards, and reward employees for practicing security. These rewards include special recognition, bonuses for hitting targets, and promotion opportunities.

CIOs must also assess risks and build security portals for emergency response. In addition, the state CIOs should develop model state legislation to protect confidentiality in reporting security breaches and responses to them. The legislation should allow for the sharing of information among government entities. There also should be federal support for establishing an interstate ISAC.

The 10 recommendations that comprise this call to action reflect the belief that we cannot simply declare that everything has changed since September 11th. We must *take action* to change some of the ways we live and conduct business. We must build a world that protects our loved ones and the critical assets we all require to sustain our way of life.

Appendix I: Report from the NASCIO Forum on Security and Critical Infrastructure Protection

by Chris Dixon, NASCIO Digital Government Issues Coordinator

November 13-14, 2001
Dulles Airport Marriott
Washington, D.C.

Introduction

Security as it relates to information technology (IT)—often referred to as cyber-security—represents the ability of electronic-information owners to assure the following aspects of information systems.

- Confidentiality—information is accessible only to authorized parties.
- Integrity—information is accurate and complete at all times.
- Availability—systems are accessible and can deliver information when needed.

Secure information systems are as vital to citizen trust in digital government transactions as they are to consumers in electronic commerce. Moreover, governments attempting to do business online must comply with complicated privacy laws that can treat multiple instances of the same citizen information differently in various contexts depending on where the information is collected and how it is used. This adds to the complexity of security measures to defend information systems against the following threats.

- Insiders—accidental or malicious compromises of security protocols by authorized users
- Crackers/Virus Writers—random individuals seeking to penetrate or disable systems for personal satisfaction
- Activists—issue-oriented individuals seeking to penetrate or disable systems on behalf of a cause
- Organized Criminals—groups seeking to penetrate or disable systems for profit
- Terrorists—groups seeking to penetrate or disable systems in order to exacerbate the effects of violent acts
- Spies—intelligence operatives seeking to penetrate or disable systems on behalf of commercial or political interests
- Information Warriors—military forces seeking to penetrate or disable systems as part of a larger conflict among nation states

Toward addressing these goals and issues, the National Association of State Chief Information Officers (NASCIO) sponsored the Forum on Security and Critical Infrastructure Protection. More than 80 individuals participated in the day-and-a-half event. Participants included state CIOs and security chiefs representing 35 states. Other participants included representatives of local and federal government IT management as well as staff from other agencies and branches of state government. (Forum presentations can be found online on NASCIO's website at www.nascio.org/2001/11/securityforum011113-14.cfm.)

State CIOs have found that cyber-threats to state-government IT systems, including cyber-terrorism, have not become more pronounced since the recent War on Terrorism began in response to the September 11th attacks. (This is likely due to the fact that Islamic jihadists have not invested resources in this area.) However, thanks to sources such as Carnegie Mellon's CERT/CC, state CIOs are acutely aware of the fact that, over time, all types of cyber-threats are likely to increase in frequency and sophistication, with different threats emerging at different times from disparate sources worldwide. Fortunately, public interest in assuring the availability of government services (and, thus, the IT that supports them) has risen along with interest in assuring other aspects of the nation's critical infrastructure such as power, water, communication, financial, and transportation services, among others. Additionally, public officials are increasingly aware of the need to share reliable information as part of defense and emergency management efforts in times of crisis.

This report is the product of the forum. It provides a series of recommendations and action items under the headings of architecture, assessment, business alignment, education and communication, funding, governance, and legislation. Some of the action items are directed toward the states and others will be carried out by NASCIO and its organizational partners, including the National Governors' Association (NGA) and the federal government, among others.

Governance

Assuring public safety and the reliability of public services is a fundamental function of government. Toward that end, security oversight must be formally and permanently installed at the executive level of state government. Furthermore, the IT security governance structure must span the branches of government and include city and county participation.

State Action:

- Define and implement an adaptable governance structure for IT security.
- Link local governments into the governance process.

NASCIO Actions:

- Collect progressive governance practices for use by the states.
- Serve as an active voice for the states at the federal level.
- Coordinate efforts with the National League of Cities (NLC), the National Association of Counties (NACo), and NGA to aggressively promote governance models and best practices.

State and NASCIO Actions:

- Promote the fact that (1) IT is integral to prevention and response, (2) citizens hold government to a higher standard of privacy/security than the private sector, and (3) security can no longer be "delegated" to IT exclusively.
- Articulate a vision of what needs to be accomplished.

Legislation

Establishing a permanent, high-profile role for cyber-security will require legislative action and statutory authority. A governance body will have to be formally established. Security standards will have to be assessed and enforced. All of this will require the sponsorship of governors and key legislators who have to educate their peers on the nuances of cyber-security and technology. (Biometrics are not a cure-all!) State CIOs and their security chiefs will have to impress upon policy makers that cyber-security is an integral part of physical security and homeland defense.

State Actions:

- Statutorily identify an entity with compliance and enforcement authority over enterprise IT management, including security.

- Support the passage of legislation that would exempt state cyber-security communications with the federal government and ISACs from FOIA/Open Access laws—and encourage states to pass similar legislation to foster appropriate internal sharing and interchange with private partners regarding critical infrastructure.
- Keep all cyber-security legislation broad in regard to cyber-threats, not limited to cyber-terrorism.
- Champion legislation that creates real penalties for cyber-crimes of all varieties.

NASCIO Actions:

- Circulate examples of IT-management legislation that establishes security compliance and enforcement authority through a variety of centralized and decentralized arrangements.
- Conduct a grassroots campaign among the states to support federal cyber-security legislation that benefits the states.
- Educate governors, state CIOs, legislators, and commissioners of uniform state laws about the need for cyber-security legislation.
- Work with the National Conference of Commissioners of Uniform State Laws (NCCUSL) to draft model legislation that allows appropriate and confidential internal sharing of security-related information within and among the branches of state government and with private partners.
- Issue a background paper and talking points with the National Center for State Courts (NCSC), the National Conference of State Legislators (NCSL), NCCUSL, and NGA apprising policy makers of the need for legislation.

Business Alignment

In order to make security more than just an afterthought, or a series of procedures and technologies that are merely bolted on to existing operations, state CIOs and other policy makers will have to recognize it as an integral element of any digital-government rollout. Officials must be able to point to a specific set of critical business offerings—for example, public safety, education, human services, finances, and e-commerce—that depend on reliable computing and communication systems and assign security resources accordingly. These essential services will also be seen as the juiciest targets for attack, as bringing them down will deliver the heaviest blows to governments and citizens. Moreover, as citizens seek a more unified digital-government presentation that spans all the levels of government, state CIOs and their security chiefs will need to coordinate with local and federal service providers to eliminate seams that invite cyber-threats to divide and conquer with attacks on the weakest link.

State Actions:

- Collaborate with local and federal government on issues of continuity and security.
- Include security as a part of planning for IT systems.
- Synchronize security and business-continuity plans across jurisdictions and levels of government.
- Act with a sense of urgency!

NASCIO Actions:

- Ensure federal, state, and local collaboration.
- Facilitate public-private relationships that will help identify the best solutions for security and business continuity.
- Facilitate communication to the public at large.

Assessment

Establishing standards for security and incorporating them into the enterprise architecture will be only an intermediate step in the process. Determining those security standards will require an assessment of the likely threats to state IT assets along with the corresponding risks—that is, the pain that will be suffered as a result of a particular violation. This will, in turn, allow security architects to prescribe particular security standards that meet at the intersection of a likely cyber-threat and the level of risk a given owner can reasonably (or legally) tolerate. Moreover, assessments will have to be conducted periodically to check and enforce compliance with security standards across the enterprise if these standards are to be more than just friendly suggestions.

State Actions:

- Adopt a common state-federal methodology for identifying and assessing critical assets—for example, the Critical Infrastructure Assurance Office's U.S. Project Matrix. This methodology, focusing on mission-critical business processes, should identify interdependencies among internal and external systems and identify risks and vulnerabilities.
- Conduct assessments utilizing a joint state-federal assessment tool.
- Develop a business case to drive response to identified risks and vulnerabilities—quantify the cost of not acting in order to make inaction untenable.
- Coordinate state and federal homeland security efforts toward critical infrastructure assurance.
- Report best practices and success stories back to NASCIO.

NASCIO Actions:

- Act as a clearinghouse for progressive practices and success stories.
- Develop a business case for assessment.
- Help to align national assessment efforts among states and across the levels of government.
- Work with NGA to present a common voice in pursuit of federal funding support.
- Encourage the federal government to coordinate intergovernmental assessment efforts through the Office of Homeland Security.

Architecture

An adaptive, enterprise information architecture provides a set or framework of agreed-upon principles and standards, based upon business processes, that enable information sharing and interoperability across the enterprise. These enterprise-wide standards, incorporating fundamental security and privacy concerns, allow numerous departments and agencies to develop systems that meet universal requirements without forcing them to deploy a particular product or a specific technology type. Enterprise-wide adoption of architectural standards is an ongoing process of definition and education. It is not a one-time project or initiative. Over time, the coherent development of dispersed systems will facilitate sharing of information, and it will permit security personnel to better manage ever changing systems and capitalize on what should be a real home-field advantage against cyber-threats.

State Actions:

- Endorse the forthcoming NASCIO *Enterprise Architecture Toolkit* and commit resources to make architecture a high priority.
- Define your enterprise and identify your stakeholders, recognizing that stakeholders are not just internal, but span disciplines, jurisdictions, and branches of government.
- Establish a governance structure that effectively manages the architecture.
- Provide real leadership, not just mandates, in architecture for local units of government.

NASCIO Actions:

- Publish *Enterprise Architecture Toolkit* for the states.
- Promote the development of compatible architecture among the states that will enable information sharing and interoperability.
- Play a leadership role with respect to awareness, education, and adoption of architecture.
- Serve as a repository of effective architectural practices from government and private industry.

Education and Communication

Long-term cyber-security will require education to raise America's consciousness of cyber-threats and prevention. Targeted messages and instructions will have to be delivered to everyone from citizens (who should be able to recognize and report cyber-crimes) to state employees (who must be vigilant against lapses and violations of procedures and systems) to policy makers (who must be apprised of the nature and limitations of various security strategies and technologies before implementing them). State CIOs and their security chiefs should be prepared to formulate internal security education programs and champion external security education programs. Specific cyber-security and critical-infrastructure-protection campaigns will have to be developed for the different levels of government as well as for citizens and other private-sector partners. Over time, messages should be tailored to address immediate and emerging threats as identified through intergovernmental communication (horizontal and vertical) of incident-related data and alerts.

State Actions:

- Identify key stakeholders.
- Develop a cyber-security and critical-infrastructure-protection education curriculum.
- Develop information sharing mechanisms between the state, local governments, and private entities.

NASCIO Actions:

- Develop a cyber-security and critical-infrastructure-protection education framework.
- Act as a conduit to the federal government, allowing the states to speak with one voice.
- Establish a state security information sharing and analysis center (interstate ISAC) to facilitate communication among the states and the federal government.

Funding

As security is a fundamental concern for IT, funding for security must reflect its importance to the reliability of citizen-centric digital government. This will mean the strategic and rapid deployment of expertise, training, and technologies to secure critical business processes across the enterprise. Funding must be deployed flexibly within an enterprise, not a stovepipe, view, allowing resources to flow to where they are needed most immediately. Ongoing research and development will also play a key role in countering immediate and emerging cyber-threats. State government will routinely call upon existing resources at the universities and in the private sector to supplement internal resources.

State Actions:

- Include funding for certification and validation of cyber-security, disaster-recovery, and business-continuity standards.
- Assign responsibility for enterprise cyber-security funding within the state IT governance structure.

NASCIO Actions:

- Work with NGA to identify a single federal contact who can help eliminate barriers in federal stovepipe funding.
- Explore all potential sources of funding and technical assistance.
- Act as a clearinghouse for funding strategies at state, local, and federal levels.

Forum Participants

Steve Akridge
Georgia

Kim Bahrami
Florida

Claire Bailey
Arkansas

David Ballard
Kentucky

Jean Bogue
NASCIO/NSR

Howard Boksenbaum
Rhode Island

Dave Boyer
U.S. Department of Justice

Mike Boyer
Montana

Andy Cannon
Alabama

Mary F. Carroll
Ohio

Joe Christensen
Georgia

Keith Comstock
West Virginia

Steven Correll
NLETS

Elias S. Cortez
California

John Curley
NASCIO/NSR

Sharon Dawes
Center for Technology in Government

Matthew R. DeZee
South Carolina

Chris Dixon
NASCIO

Allen L. Doescher
Louisiana

Otto Doll
South Dakota

Greg Dzieweczynski
Minnesota

Cheryl Edwards
NASCIO

Donald Evans
Public Technology, Inc.

Bob Feingold
Colorado

David Fisher
Minnesota

Frank Galeotos
Wyoming

Ann Garrett
North Carolina

Charles F. Gerhards
Pennsylvania

Danielle M. Germain
ITAA

Curt Haines
Pennsylvania

Lynn Harris
New Mexico

Ron P. Hawley
North Carolina

John Hohl
Wyoming

Laura Iwan
New York

Leon Jackson, Jr.
District of Columbia

Thomas M. Jarrett
Delaware

Larry G. Kettlewell
Kansas

George Kohut
Public Technology, Inc.

Laura Larimer
Indiana

Erin Lee
National Governors' Association

Steven Lee
West Virginia

Vic Mangrum
Tennessee

Chad C. McGee
Louisiana

Valerie J. McNevin
Colorado

Scott McPherson
Florida

Michael McVicker
Washington

Elizabeth Miller
NASCIO

Amy Moran
Wisconsin

Gail A. Morris
Missouri

Kym Patterson
Arkansas

William F. Pelgrin
New York

Holli I. Ploog
DynCorp Management Resources, Inc.

R. D. Porter
Missouri

Jim Pritchett
National Center for State Courts

Susan Puntillo
Wisconsin

Carolyn T. Purcell
Texas

Wendy W. Rayner
New Jersey

Rock Regan
Connecticut

Mark Reynolds
Connecticut

David J. Roberts
SEARCH

Gary Robinson
Washington

Beth Roszman
NASCIO

Thom Rubel
National Governors' Association

Terry Savage
Nevada

Steve Schafer
Nebraska

N. Jerry Simonoff
Virginia

Dan Sipes
North Dakota

Craig Stender
Arizona

Marianne Swanson
NIST

Matthew Trail
NASCIO

Donald W. Upson
Virginia

Aldona K. Valicenti
Kentucky

Randall von Liski
Illinois

Richard C. Webb
PricewaterhouseCoopers, LLP

Gerry Wethington
Missouri

Mary Gay Whitmer
NASCIO

Rick Zelznak
Arizona

Appendix II: Mark's Story: A Hypothetical Case Study

The CIO Responds

It was winter in the heartland. Mark, a senior technologist for his state government's Unix-derived operating systems, was ready to go home. Before leaving, he decided to conduct one last check of the operating system that supports the state's Department of Natural Resources' server applications. The department's system was recently moved to Mark's central server farm. While checking the health of the system he noticed that an obscure operating system file had been updated only an hour earlier. Mark was puzzled, as he had not applied any fixes or patches that day.

When Mark examined the changed file, he saw that the code was capable of spying on password traffic that moved across a local area network (LAN) segment. The code was thin and looked like a dormant agent. Mark realized the system had been hacked. This hack was deep and the intent was clear. The LAN segment included a central payment system. If this system was compromised, Mark knew vital state operations could be seriously impaired.

He immediately notified his management, the state CIO, and the state chief security officer. The departmental owners of the systems were also notified. In short order, the LAN segment was reconfigured and the affected systems were re-certified by the owners. Mark and the chief security officer documented the intrusion and attempted to understand how the hacker was able to penetrate the state's security infrastructure. The State Bureau of Investigations (SBI) was called in to assist in the analysis. More than 10 days of investigation passed with no clear results.

As it turned out, the hack Mark discovered was particularly nasty. Ron, the state's CIO, was concerned that the initial investigation of the hack yielded no information about how it occurred. Ron was hoping for additional information before he briefed the state's Security Council. Immediately after the hack, Ron met with the state's chief IT architect and the chief security officer to discuss the hack and the steps that would be followed to flush the hack and investigate how it happened. During the meeting, the chief security officer commented, "A hack of this nature is worth about $8,000." Ron was taken aback. "Are people selling these hacks?" he asked. The answer was swift and direct, "Yes."

As Ron worked on his briefing for the IT Security Council, he wondered to himself: *Are there agents inside our operations and we just don't know about them? Maybe I am dealing with a much larger problem here*.

Fortunately, Ron worked in a state that has a strong IT governance structure. The structure includes an executive-level policy council for IT as well as support organizations for e-government, geographic information systems, and security. The Security Council is a key support organization with IT stakeholder members from the audit community, emergency management, and security staff in state agencies. Ron is very proud of the council's work and its enterprise representation. Nonetheless, he knew the briefing would be difficult.

The Enterprise Responds

Before Ron briefed the Security Council, he asked Mark to re-platform the Department of Natural Resources application on a new server and leave the old server intact for the investigation. This proved to be a very important decision.

Ron then hired a security consultant to investigate the server and application. The consultant learned that the hack occurred in two stages. The first stage happened before the server was moved to Mark's server farm. During this stage the hacker created a back-door path to the server. After the server moved to Mark's area, the hacker came back and created a routine to spy on LAN traffic. The consultant also discovered how the hacker navigated to the server when it was located in the Department of Natural Resources and he discovered how the hacker got into Mark's LAN. The security holes he discovered were immediately closed. Ron included this information in his security briefing notes.

He also included in his notes information from the security log kept by Mark. A day before the briefing, Ron met with the consultant to discuss how well the agencies document security breaches and how well they follow the state's IT security architecture. The meeting was disappointing. Agencies do not always follow the architecture for old infrastructure and applications. However, they meticulously follow the architecture for new infrastructure and applications. Also, the consultant confirmed that agencies do not keep meaningful metrics on security intrusions, successful penetrations, down time, and the like. The Security Council briefing was scheduled for 1:00 p.m.

The Security Council was formed the previous year in response to Ron's concerns about the growing number of intrusions the state was observing in the network. The number increased an alarming 25 percent in a three-month period. Ron also wanted the state to take a more aggressive approach to handling viruses and spams. He created a Constant Readiness Center to handle disaster recovery, and he wanted the center to expand its role to include coordination of emergency responses to viruses and other homeland security cyber-threats. Emergency management staff from the Adjutant General's Office was formally invited to join the Security Council and to provide staff for the Constant Readiness Center.

Ron knew the Security Council and the Constant Readiness Center staff would have many questions about Mark's hacker and would wonder about how many undetected agents could conceivably be residing in the state's systems. During the meeting, the council talked about security risks, noting that half of the security violations reported to the FBI and the Systems Administration, Networking, and Security Institute were violations perpetrated by insiders. The council asked Ron how the state controls against insider attacks and how the state protects itself from outsiders "social engineering" key staff to disclose security passwords, architectures, and techniques for safeguarding critical infrastructure.

When Ron told the council that agencies were following the security architecture for new infrastructure but not always using it for old infrastructure or applications, Janet, the chief security officer for the Department of Labor, made an important observation. "We need to conduct a statewide inventory of all our systems," she said. "We can use our Y2K inventory and update it with a security assessment." Janet volunteered to head a subcommittee to develop a "simple and practical" assessment methodology. "The methodology will point to our vulnerabilities. We can then use our architecture to fix the most critical vulnerabilities."

This discussion extended into a dialogue about security audit standards. The council decided to explore national audit standards and craft a policy statement for consideration by the executive IT policy council to train state employees on the standards. The council also drafted a recommended policy for building the standards into position profiles and job class specifications. The council reasoned that IT audit standards, risk assessments, and architecture can drive security metrics, since they are all tied together. A second subcommittee was created to recommend the audit standards that would be adopted by the entire enterprise.

Ron then told the council how the state had failed when it moved the Department of Natural Resources server to Mark's area. Ron explained that when the server was moved, it was placed on the next available LAN segment without regard to other systems on the segment. Mark did not do the move. Instead, a unit that performs facilities management services did the move. The technologist who handled the move assumed the security infrastructure on the LAN segment would protect against outside intrusions, and was not aware a back door existed prior to the move. Also, the server was not evaluated for abnormalities before it was moved and management did not oversee the move. The meeting with the Security Council lasted over four hours.

Lessons Learned

After briefing the Security Council, Ron—the state's CIO—scheduled a meeting with the Constant Readiness Center staff. Ron knew that it was impossible to parse every intrusion. His staff was small and his budget limited. The Readiness Center team understood Ron's money concerns; however, they felt providing security analysis services to state agencies and local units of government for a subscription fee could solve the problem. Also, they felt Ron could seek federal help through emergency management grants to cover start-up costs. Ron was intrigued with the suggestions. Clearly an analysis center would help disseminate information, provide technical security support to agencies, and serve as a clearinghouse and reporting organization for metrics and vulnerability assessments. The Readiness Center staff agreed to review their mission and propose an expanded role. The staff also recommended that the Readiness Center create a security lab to investigate emerging technologies, especially those that are more offensive in nature.

Ron knew the recommendations from the Security Council and Readiness Center would be expensive. He remembered back a year ago when he contracted with a national firm for a full-time network engineer. The engineer was an expert who for one year worked on site directly with state network technologists to develop a highly hardened network infrastructure. While the expert cost $155,000 per year, he was worth every cent. Ron's network up-time reports exceeded "four nines" (i.e., 99.99 percent)—quite an accomplishment in an 830-router network. Ron's customer satisfaction ratings were equally impressive—more than meeting expectations on performance, communication, price value, and understanding customer business needs. Ron remembered back four years when the satisfaction scores were only 78 percent of expectation. However, when the budget reductions came, Ron decided to cut the expert. This was a hard choice to make, but he saw few alternatives. The hacker and funding concerns were constantly on Ron's mind.

Mark—the state senior technologist—and Ron faced a unique challenge. They never caught the hacker, but they did safeguard their state's critical systems. Ron implemented a security analysis center, adopted COBIT audit standards, and built the audit standards into all IT position profiles and job class specifications. He leveraged his governance structure to help fund the security initiatives. Over 150 professionals were trained in COBIT, and the agencies gladly paid for the training. The state auditors developed a security risk assessment methodology and used it in their agency audit work. The audit standards, risk assessment, and analysis center work drove performance metrics. Funds were raised to begin work on a security portal, and legislation was passed to protect the confidentiality of security breaches and unwelcome intrusions. Most importantly, for over six months there have been no reported security breaches in any of the state agencies.

It was snowing in the heartland when Mark first encountered the hacker. Today, it is spring in the heartland, about 3:30 in the afternoon. Ron's phone is ringing. It is Mark and he is excited. "Ron, the hacker is back and I can see him trying to get into my honey pot." Ron laughed the low kind of laugh that comes when you are satisfied. "This is great," Ron declared. "Go get him!"

It took some time for Ron to completely realize the full significance of Mark's experience with the hacker. Ron was aware of the thousands of hits reported each week from intrusion-detection software. However, few hits ever materialized into a hack or penetration. Over time the thousands of hits were only bumps in the night to Ron. Yet one of the bumps was very real and serious. Ron wondered: *What about all those other bumps?* As Ron reflected he came to a new understanding. He realized the bumps are all real. *People want to get into my state's systems. They are out there and they are* *probing us*. Ron thought: *Each bump has a purpose*. This realization gave Ron pause and he experienced a metanoia: *I am part of a larger world, bigger than just my state. How many other states have been exploited in this way? How many exploits like this have gone unnoticed until it was too late? How could CIOs share and learn from experiences like this?*

Catching Mark's hacker before he does damage is a single success—a loud bump in the night. Ron had a change of heart. He realized that his state needed to help and to receive help from other states. Ron realized that security is a way of life that demands aggressive action tempered by humility and a willingness to share.

Appendix III: Recommended Resources

Center for Technology in Government
(State University of New York at Albany)

- Project: "Sharing the Costs, Sharing the Benefits: The NYS GIS Cooperative" www.ctg.albany.edu/projects/gis/gismenu.html

Computer Science and Telecommunications Board
(The National Academy of Science)

- Publications—Topic: Security, Assurance and Privacy www4.nas.edu/cpsma/cstb.nsf/web/topic_security
- "Summary of a Workshop on Information Technology Research for Crisis Management" www4.nationalacademies.org/cpsma/cstb.nsf/web/pub_crisismanagement

Dartmouth College

- Institute for Security Technology Studies www.ists.dartmouth.edu

IT Governance Institute

- "Board Briefing on IT Governance" (www.itgi.org)
- "Information Security Governance: Guidance for Boards of Directors and Executive Management (www.itgi.org)

National Institute for Standards and Technology (NIST)

- Computer Security Resource Center csrc.nist.gov

RAND

- "Research on Mitigating the Insider Threat to Information Systems—#2: Proceedings of a Workshop Held August, 2000" www.rand.org/publications/CF/CF163
- "Security Controls for Computer Systems" www.rand.org/publications/R/R609.1/R609.1.html

U.S. Commission on National Security/21st Century (The Hart-Rudman Commission)

- Final Phase III Report—"Road Map For National Security: Imperative for Change" www.nssg.gov

Endnotes

1. Richard Clarke, Keynote Address, *Conference on Critical Infrastructures: Working Together in a New World*, 12 February 2002, Austin, Texas (notes of Chris Dixon, conference attendee).

2. Jeffery Eisenach, Thomas Lenard, and Stephen McGonegal, *The Digital Economy Fact Book* (3rd edition, 2001), (Washington, D.C.: Progress and Freedom Foundation), 1-9.

3. Ibid., 24-27.

4. National Governors' Association, "Homeland Security: The Cost to States for Ensuring Public Health and Safety," *Issue Brief*, 5 December 2001, <http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_2915,00.html> (20 March 2002).

5. Barbara Gomolski, Jeremy Grigg, and Kurt Potter, "2001 IT Spending and Staffing Survey Results," *Gartner Group Strategic Analysis Report* R-14-4158, 19 September 2001, 9.

6. James Middleton, "Major viruses cost industry $13bn in 2001," *vnunet.com*, 10 January 2002, <http://www.vnunet.com/News/1128147> (20 March 2002).

7. Andy Briney, "Cover Story: 2001 Industry Survey," *Information Security*, October 2001, <http://www.infosecuritymag.com/articles/october01/images/survey.pdf> (21 March 2002), 34-43.

8. Harold Leavitt, "Applied Organizational Change in Industry: Structural, Technological, and Humanistic Approaches," *Handbook of Organizations* (J.G. March, ed.), (Chicago: Rand McNally, 1965), 1144-1170.

9. Allen Hutt, *Open framework: Transforming Your Business with Information Technology* (Issue 1), November 1994, (Bracknell Berks, England: International Computers Limited), 1-8.

10. For a broad discussion of the attributes of digital government, see NASCIO's publication "Creating Citizen-Centric Digital Government: A Guide for the States" at <http://www.nascio.org/hotissues/dg>.

11. Thanks to John W. Lainhart IV, the first Inspector General of the U.S. House of Representatives, a member of the COBIT Steering Committee, for his assistance in editing the following section on COBIT.

12. John W. Lainhart IV, "Assuring Service Improvements and Systems Modernization," slide presentation for PricewaterhouseCoopers, LLP, October 2001.

13. IT Governance Institute, "Executive Summary," *COBIT Governance, Control and Audit for Information and Related Technology* (3rd ed.), July 2000, <http://www.itgi.org/resources.htm> (20 March 2002), 6.

14. NIST, "Federal Information Technology Security Assessment Framework" 28 November 2000, <http://www.cio.gov/Documents/federal_it_security_assessment_framework_112800.html> (16 April 2002).

15. Stephen R. Covey, *The Seven Habits of Highly Effective People* (New York: Simon and Schuster, 1990).

16. Ibid., 95-144.

17. William Welsh, "IT security regulations unlikely, Bush official says," *Washington Technology*, 8 April 2002, <http://www.washingtontechnology.com/news/1_1/state/18080-1.html> (30 April 2002).

18. Victor H. Vroom, *Work and Motivation* (New York: John Wiley and Sons, 1964).

ABOUT THE AUTHOR

Don Heiman recently retired from the State of Kansas, where he served four years as the chief information technology officer for the executive branch and chief information technology architect for the three branches of government. During his tenure, Kansas was widely regarded as a national leader in digital government innovation and implementation. For the past seven years, Heiman also directed the state's central data center and the wide area network used by Kansas state agencies. He began his career in state government in 1976 with the Kansas Legislative Division of Post Audit, where he directed the performance and IT audit staffs.

Prior to joining the state, Heiman worked for Midwest Research Institute in Kansas City, Missouri, as an industrial economist. He also worked as a personnel officer and later as Board of Trustees consultant for North Kansas City Memorial Hospital. He was drafted into the U.S. Army in 1971. During his active duty at Fort Gordon, Georgia, he served in the Army's medical corps as a social work specialist E-5.

He is the author of numerous articles and papers in academic journals both in the United States and England. He served seven years on the editorial board for the *Journal of Organizational Change Management.*

Heiman holds an undergraduate degree in business from Rockhurst University in Kansas City, a master of science in business from the University of Kansas, a master of arts in pastoral studies from Loyola University (New Orleans), and master of public administration from the Edwin O. Stene School of Public Administration at the University of Kansas.

KEY CONTACT INFORMATION

To contact the National Association of State Chief Information Officers:

Mr. Chris Dixon
NASCIO
167 West Main Street, Suite 600
Lexington, KY 40507-1324
(859) 231-1971
fax: (859) 231-1928

e-mail: nascio@amrinc.net (general inquiries)
website: www.nascio.org

GRANT REPORTS

E-Government

Managing Telecommuting in the Federal Government: An Interim Report (June 2000)

Gina Vega
Louis Brennan

Using Virtual Teams to Manage Complex Projects: A Case Study of the Radioactive Waste Management Project (August 2000)

Samuel M. DeMarie

The Auction Model: How the Public Sector Can Leverage the Power of E-Commerce Through Dynamic Pricing (October 2000)

David C. Wyld

Supercharging the Employment Agency: An Investigation of the Use of Information and Communication Technology to Improve the Service of State Employment Agencies (December 2000)

Anthony M. Townsend

Assessing a State's Readiness for Global Electronic Commerce: Lessons from the Ohio Experience (January 2001)

J. Pari Sabety
Steven I. Gordon

Privacy Strategies for Electronic Government (January 2001)

Janine S. Hiller
France Bélanger

Commerce Comes to Government on the Desktop: E-Commerce Applications in the Public Sector (February 2001)

Genie N. L. Stowers

The Use of the Internet in Government Service Delivery (February 2001)

Steven Cohen
William Eimicke

State Web Portals: Delivering and Financing E-Service (January 2002)

Diana Burley Gant
Jon P. Gant
Craig L. Johnson

Internet Voting: Bringing Elections to the Desktop (February 2002)

Robert S. Done

Leveraging Technology in the Service of Diplomacy: Innovation in the Department of State (March 2002)

Barry Fulton

Federal Intranet Work Sites: An Interim Assessment (June 2002)

Julianne G. Mahler
Priscilla M. Regan

The State of Federal Websites: The Pursuit of Excellence (August 2002)

Genie N. L. Stowers

State Government E-Procurement in the Information Age: Issues, Practices, and Trends (September 2002)

M. Jae Moon

Preparing for Wireless and Mobile Technologies in Government (October 2002)

Ai-Mei Chang
P. K. Kannan

Public-Sector Information Security: A Call to Action for Public-Sector CIOs (October 2002, 2nd ed.)

Don Heiman

Financial Management

Credit Scoring and Loan Scoring: Tools for Improved Management of Federal Credit Programs (July 1999)

Thomas H. Stanton

Using Activity-Based Costing to Manage More Effectively (January 2000)

Michael H. Granof
David E. Platt
Igor Vaysman

Audited Financial Statements: Getting and Sustaining "Clean" Opinions (July 2001)

Douglas A. Brook

An Introduction to Financial Risk Management in Government (August 2001)

Richard J. Buttimer, Jr.

Human Capital

Profiles in Excellence: Conversations with the Best of America's Career Executive Service (November 1999)

Mark W. Huddleston

Leaders Growing Leaders: Preparing the Next Generation of Public Service Executives (May 2000)

Ray Blunt

Reflections on Mobility: Case Studies of Six Federal Executives (May 2000)

Michael D. Serlin

A Learning-Based Approach to Leading Change (December 2000)

Barry Sugarman

Labor-Management Partnerships: A New Approach to Collaborative Management (July 2001)

Barry Rubin
Richard Rubin

Winning the Best and Brightest: Increasing the Attraction of Public Service (July 2001)

Carol Chetkovich

Organizations Growing Leaders: Best Practices and Principles in the Public Service (December 2001)

Ray Blunt

A Weapon in the War for Talent: Using Special Authorities to Recruit Crucial Personnel (December 2001)

Hal G. Rainey

A Changing Workforce: Understanding Diversity Programs in the Federal Government (December 2001)

Katherine C. Naff
J. Edward Kellough

Life after Civil Service Reform: The Texas, Georgia, and Florida Experiences (October 2002)

Jonathan Walters

Managing for Results

Corporate Strategic Planning in Government: Lessons from the United States Air Force (November 2000)

Colin Campbell

Using Evaluation to Support Performance Management: A Guide for Federal Executives (January 2001)

Kathryn Newcomer
Mary Ann Scheirer

Managing for Outcomes: Milestone Contracting in Oklahoma (January 2001)

Peter Frumkin

The Challenge of Developing Cross-Agency Measures: A Case Study of the Office of National Drug Control Policy (August 2001)

Patrick J. Murphy
John Carnevale

The Potential of the Government Performance and Results Act as a Tool to Manage Third-Party Government (August 2001)

David G. Frederickson

Using Performance Data for Accountability: The New York City Police Department's CompStat Model of Police Management (August 2001)

Paul E. O'Connell

Performance Management: A "Start Where You Are, Use What You Have" Guide (October 2002)

Chris Wye

New Ways to Manage

Managing Workfare: The Case of the Work Experience Program in the New York City Parks Department (June 1999)

Steven Cohen

New Tools for Improving Government Regulation: An Assessment of Emissions Trading and Other Market-Based Regulatory Tools (October 1999)

Gary C. Bryner

Religious Organizations, Anti-Poverty Relief, and Charitable Choice: A Feasibility Study of Faith-Based Welfare Reform in Mississippi (November 1999)

John P. Bartkowski
Helen A. Regis

Business Improvement Districts and Innovative Service Delivery (November 1999)

Jerry Mitchell

An Assessment of Brownfield Redevelopment Policies: The Michigan Experience (November 1999)

Richard C. Hula

Determining a Level Playing Field for Public-Private Competition (November 1999)

Lawrence L. Martin

San Diego County's Innovation Program: Using Competition and a Whole Lot More to Improve Public Services (January 2000)

William B. Eimicke

Innovation in the Administration of Public Airports (March 2000)

Scott E. Tarry

Entrepreneurial Government: Bureaucrats as Businesspeople (May 2000)

Anne Laurent

Implementing State Contracts for Social Services: An Assessment of the Kansas Experience (May 2000)

Jocelyn M. Johnston
Barbara S. Romzek

Rethinking U.S. Environmental Protection Policy: Management Challenges for a New Administration (November 2000)

Dennis A. Rondinelli

The Challenge of Innovating in Government (February 2001)

Sandford Borins

Understanding Innovation: What Inspires It? What Makes It Successful? (December 2001)

Jonathan Walters

A Vision of the Government as a World-Class Buyer: Major Procurement Issues for the Coming Decade (January 2002)

Jacques S. Gansler

Contracting for the 21st Century: A Partnership Model (January 2002)

Wendell C. Lawther

Franchise Funds in the Federal Government: Ending the Monopoly in Service Provision (February 2002)

John J. Callahan

Managing "Big Science": A Case Study of the Human Genome Project (March 2002)

W. Henry Lambright

Leveraging Networks to Meet National Goals: FEMA and the Safe Construction Networks (March 2002)

William L. Waugh, Jr.

Government Management of Information Mega-Technology: Lessons from the Internal Revenue Service's Tax Systems Modernization (March 2002)

Barry Bozeman

Making Performance-Based Contracting Perform: What the Federal Government Can Learn from State and Local Governments (June 2002)

Lawrence L. Martin

21st-Century Government and the Challenge of Homeland Defense (June 2002)

Elaine C. Kamarck

Moving Toward More Capable Government: A Guide to Organizational Design (June 2002)

Thomas H. Stanton

Transforming Organizations

The Importance of Leadership: The Role of School Principals (September 1999)

Paul Teske
Mark Schneider

Leadership for Change: Case Studies in American Local Government (September 1999)

Robert B. Denhardt
Janet Vinzant Denhardt

Managing Decentralized Departments: The Case of the U.S. Department of Health and Human Services (October 1999)

Beryl A. Radin

Transforming Government: The Renewal and Revitalization of the Federal Emergency Management Agency (April 2000)

R. Steven Daniels
Carolyn L. Clark-Daniels

Transforming Government: Creating the New Defense Procurement System (April 2000)

Kimberly A. Harokopus

Trans-Atlantic Experiences in Health Reform: The United Kingdom's National Health Service and the United States Veterans Health Administration (May 2000)

Marilyn A. DeLuca

Transforming Government: The Revitalization of the Veterans Health Administration (June 2000)

Gary J. Young

The Challenge of Managing Across Boundaries: The Case of the Office of the Secretary in the U.S. Department of Health and Human Services (November 2000)

Beryl A. Radin

Creating a Culture of Innovation: 10 Lessons from America's Best Run City (January 2001)

Janet Vinzant Denhardt
Robert B. Denhardt

Transforming Government: Dan Goldin and the Remaking of NASA (March 2001)

W. Henry Lambright

Managing Across Boundaries: A Case Study of Dr. Helene Gayle and the AIDS Epidemic (January 2002)

Norma M. Riccucci

SPECIAL REPORTS

Government in the 21st Century

David M. Walker

Results of the Government Leadership Survey: A 1999 Survey of Federal Executives (June 1999)

Mark A. Abramson
Steven A. Clyburn
Elizabeth Mercier

Creating a Government for the 21st Century (March 2000)

Stephen Goldsmith

The President's Management Council: An Important Management Innovation (December 2000)

Margaret L. Yao

Toward a 21st Century Public Service: Reports from Four Forums (January 2001)

Mark A. Abramson, Editor

Becoming an Effective Political Executive: 7 Lessons from Experienced Appointees (January 2001)

Judith E. Michaels

The Changing Role of Government: Implications for Managing in a New World (December 2001)

David Halberstam

BOOKS*

E-Government 2001
(Rowman & Littlefield Publishers, Inc., 2001)

Mark A. Abramson and
Grady E. Means, editors

Human Capital 2002
(Rowman & Littlefield Publishers, Inc., 2002)

Mark A. Abramson and
Nicole Willenz Gardner, editors

Innovation
(Rowman & Littlefield Publishers, Inc., 2002)

Mark A. Abramson and
Ian Littman, editors

Leaders
(Rowman & Littlefield Publishers, Inc., 2002)

Mark A. Abramson and
Kevin M. Bacon, editors

Managing for Results 2002
(Rowman & Littlefield Publishers, Inc., 2001)

Mark A. Abramson and
John Kamensky, editors

Memos to the President: Management Advice from the Nation's Top Public Administrators (Rowman & Littlefield Publishers, Inc., 2001)

Mark A. Abramson, editor

Transforming Organizations
(Rowman & Littlefield Publishers, Inc., 2001)

Mark A. Abramson and
Paul R. Lawrence, editors

* Available at bookstores, online booksellers, and from the publisher (www.rowmanlittlefield.com or 800-462-6420).

About the Endowment

Through grants for research, the IBM Endowment for The Business of Government stimulates research and facilitates discussion on new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

Founded in 1998, the Endowment is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Endowment focuses on the future of the operation and management of the public sector.

For additional information, contact:
Mark A. Abramson
Executive Director
IBM Endowment for The Business of Government
1616 North Fort Myer Drive
Arlington, VA 22209
(703) 741-1077, fax: (703) 741-1076

e-mail: endowment@businessofgovernment.org
website: www.businessofgovernment.org

IBM Endowment for
**The Business
of Government**

1616 North Fort Myer Drive
Arlington, VA 22209-3195